CHIPS Magazine

April - June 2007

SHARING INFORMATION - TECHNOLOGY - EXPERIENCE




FROM THE DESKTOP TO THE BATTLEFIELD

25 YEARS
CHIPS magazine
1982 - 2007

CHIPS April - June 2007

Volume XXV Issue II

Department of the Navy Chief Information Officer
Mr. Robert J. Carey
Mr. John J. Lussier (Acting)

Space & Naval Warfare Systems Command
Commander Rear Admiral Michael C. Bachmann

Space & Naval Warfare Systems Center Charleston
Commanding Officer Captain Red Hoover

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Web support: Tony Virata DON IT Umbrella Program

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO) and the DON IT Umbrella Program Office, Space and Naval Warfare Systems Center, San Diego, Calif.

CHIPS is published quarterly by the Space and Naval Warfare Systems Center Charleston. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130.

Submit article ideas to CHIPS editors at chips@navy.mil. We reserve the right to make editorial changes. All articles printed in CHIPS become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

Requests for distribution changes or for other assistance should be directed to Editor, CHIPS, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@navy.mil; fax (757) 445-2103; DSN 565. Web address: http://www.chips.navy.mil/.

Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at chips@navy.mil or phone (757) 444-8704, DSN 564.

Features

Joint Staff Director for C4 Systems Vice Adm. Nancy E. Brown talks about ongoing initiatives in support of the joint warfighter in Iraq, Afghanistan and around the world.

Commander, 1st Battalion, 34th Armor Regiment
Army Lt. Col. John A. Nagl, a recognized authority on counterinsurgency discusses the issuance of Field Manual 3-24 - Counterinsurgency and its application to operations in Iraq and the global war on terror.

Deputy Director, Combined Joint Operations from the Sea Center of Excellence
Royal Navy Commodore Steve Cleary discusses coalition participation and interoperability in the exciting Trident Warrior 2007 series of experiments.

Commander, Navy Region Southwest
Rear Adm. Len R. Hering Sr. talks about the importance of technology in the Southwest area of operations, which encompasses six states: Arizona, New Mexico, Nevada, Colorado, Utah and California.

The crew of the experimental ship Stiletto readies the ship as it prepares to launch an unmanned aerial vehicle. The Stiletto participated in the Trident Warrior 2007 series of experiments March 20-30 aboard Naval Station Norfolk. Go to page 16 for the beginning of a series of articles about TW07. U.S. Navy photo by Photographer's Mate Airman Damien Horvath.

Navigation Guide

Editor's Notebook

The first issue of CHIPS published July 1982 as a newsletter by the Navy Regional Data Automation Center (NARDAC). It was titled Chips Ahoy and mailed to 2,500 Navy personnel. CHIPS now boasts of more than 2 million online and hardcopy readers.

Consider that in the 21st century, communications, media, information and information services will become 50 percent of America's gross national product — and its primary export — ranging from movies and television programs to music and computer software, according to reports from the U.S. Commerce Department.

With so much of America's financial security tied to information and information technology, not only do we have to do better in protecting and defending our information technology investments and intellectual capital, but we have to become even better at innovation to maintain America's role as a global giant in IT products and services.

Warfighter support to the combatant commands, security and innovation are the hallmarks of the Joint Staff Director for C4 Systems, Vice Adm. Nancy E. Brown, and her staff. Since the admiral returned to the Joint Staff in August 2006, she has issued several important documents in support of joint warfighting. The CHIPS staff and DON IT Umbrella Program team are honored to feature Vice Adm. Brown's interview as the centerpiece of the CHIPS' anniversary issue. You can read about the cutting edge changes to joint C4 systems beginning on page 6.

The Navy is a world leader in embracing and advancing new technologies. In late March, the participants of Trident Warrior 2007, the premier FORCEnet Sea Trial event, conducted a series of experiments involving about 80 technologies. The aim of the experiments is to get new capabilities into the hands of warfighters more quickly — not only for national defense, but for humanitarian relief efforts — whether here at home — or to assist neighbors in need worldwide. You can read about TW07 in a series of articles beginning on page 16.

In addition to Trident Warrior, the CHIPS staff attended the DON IM and IT Conference in February at the San Diego Convention Center. Look for CHIPS at the next DON IM and IT Conference June 18-21, 2007, at the Virginia Beach Convention Center. See the back cover for more details.

Where were you 25 years ago when CHIPS was launched? I confess, I was using a Commodore 64 or some variant at home and a Zenith at work. Yikes! The day I got a Pentium III, I thought life couldn't get much better.

Welcome new subscribers!

Sharon Anderson

By July 1987, CHIPS had undergone a name change — for obvious reasons — and began publication in magazine format. CHIPS was also published online in ASCII text and mailed over the Defense Data Network (DDN) to 250 host administrators.

In our early days, Rear Adm. Grace Hopper was a great fan of CHIPS. Hopper, co-inventor of COBOL and many other technology breakthroughs, was a pioneer and champion for bringing computer technology to the desktop in the Navy. She is shown here on our July 1986 cover with her now famous advice for pushing the envelope: "It is easier to ask for forgiveness than it is to get permission."

An issue from April 1984 featuring Zenith contract news. CHIPS has a long tradition of providing information on the best technology buys for Navy and defense customers. CHIPS' co-sponsor, the DON IT Umbrella Program, which was chartered in 1988 by the Assistant Secretary of the Navy for Financial Management, continues to bring best value pricing to Navy and defense customers.

DON CIO

Putting information to work for our people

The transformation of information technology (IT) over the past 25 years has had a significant impact on the Department of the Navy, and CHIPS Magazine has been at the forefront — reporting on the latest IT breakthroughs, policy and processes. Of course, 25 years ago, the term office automation, not information technology, was used to describe our computing environment.

Some notable changes of the past 25 years that I have witnessed during my time here at the DON include the migration of mainframe computing to desktop or personal computing. This moved the IT community from depending on the IT gurus who worked behind a glass wall to becoming the IT gurus with all the applications we needed on our own desktops.

As this migration from mainframe to desktop computing was taking place, I was involved in the Department's transition from custom solutions to commercial off-the-shelf (COTS) solutions. We went from using what was considered leading edge technologies to design, develop and build unique, full MILSPEC tactical computers and processes, to COTS and non-developmental technologies, utilizing open systems and architectures.

The reach of the DON's IT transformation continued to extend to the warfighter with the deployment of SIPRNET, our Secure Internet Protocol that got us on our way to information sharing between the warfighter and the supporting shore infrastructure. Many will attest to the fact that this is still a work in progress, but we've come a long way over the years. Adding to the sharing between the warfighter and the shore infrastructure has been the acceptance and use of the Internet as a transformational tool. Web-enabled applications have become "an accelerant" to information sharing, reachback and process improvement across the board.

The Navy Marine Corps Intranet (NMCI) gave us a new perspective and solid data on the cost of desktop computing and the proliferation of applications and networks in use across the DON. In the process of standardizing our computing environment, we took a hard look at the number of applications in use. We were surprised at the number and variety of them, but realized that we were not alone; some industry leaders found that they had an even higher number of applications.

We established Functional Area Managers who were responsible for applying a standard process to rationalize legacy applications. The result of this effort is a significantly reduced IT portfolio that provides a higher degree of efficacy. So, NMCI was a forcing function that compelled us to make some difficult decisions, but it also gave us a sense of *Enterprise*, as maintaining the DON's desktops and networks became a unified venture. With the fully trained and qualified network support staff that NMCI provided, viruses were blocked before they could strike, hackers were stopped before they could wreak havoc, and our security posture was enhanced through enterprise-wide solutions such as cryptographic logon, which was efficiently implemented for all the DON's shore-based computers.

A more recent advance that has transformed not just the DON workplace, but much of the workforce also, is the use of broadband wireless and handheld computers. Since their introduction to the DON in early 2000 as a few test devices in the DON CIO, they have become prolific throughout the Department. These devices have redefined the word mobility. It's only been a few years, but people can't imagine how they lived without them. We have just begun scratching the surface — hang on for the next 25 years!

I congratulate CHIPS for its excellence and dedication to its mission of sharing information, technology and experience, and look forward to another 25 years of CHIPS Magazine.

John J. Lussier
Department of the Navy Chief Information Officer (Acting)

DEPARTMENT OF THE NAVY - CHIEF INFORMATION OFFICER
WWW.DONCIO.NAVY.MIL

Interview with Vice Admiral Nancy E. Brown Director for C4 Systems, The Joint Staff

Vice Adm. Nancy E. Brown

Vice Adm. Nancy E. Brown serves as the Director, Command, Control, Communications and Computer Systems (C4 Systems), the Joint Staff and as the Joint Community Warfighter (JCW) Chief Information Officer (CIO). In her dual capacity she is the principal advisor to the Chairman, Joint Chiefs of Staff on all C4 systems matters within the Department of Defense (DoD) and serves as an advocate for the link between combatant commanders C4 requirements and actions to deliver capabilities to meet their needs.

Since Vice Adm. Brown returned to the Joint Staff in August 2006, she published the Joint Net-Centric Operations (JNO) Campaign Plan (available at http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf) to provide a unifying strategy to better integrate and synchronize joint community transformation and maximize joint warfighting capabilities.

This is an update to the first Joint C4 Campaign Plan, published in September 2004 by Marine Corps Lt. Gen. Robert Shea, the former Director C4 Systems, and incorporates new strategic guidance including the March 2006 National Security Strategy, the 2006 Quadrennial Defense Review Report, the 2006 Strategic Planning Guidance, the 16th Chairman's Guidance to the Joint Staff, and a new National Military Strategy for Cyberspace Operations. These documents detail the strategic direction of the Department and describe the net-centric capabilities to be employed by the joint force.

The plan also includes and builds on the significant progress in the development of net-centric concepts. Both the Net-Centric Environment (NCE) Joint Functional Concept and Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC) were approved by the Joint Requirements Oversight Council (JROC). Their approval signifies the official Department support of the operational-level net-centric capabilities required to support contingencies across the continuum of military operations, key attributes necessary to compare capability solution alternatives and how future joint force commanders (JFCs) will employ net-centric capabilities. The NCOE program has evolved into Joint Net-Centric Operations (JNO). The next version of the NCE Joint Functional Concept will be titled the "JNO Joint Functional Concept" to reflect the ongoing work to refine capabilities in the net-centric area.

Finally, the plan focuses efforts over the next two to five years on the broad goals, specific objectives and achievable actions leading to full implementation of the capabilities that Joint Net-Centric Operations provides to the joint force in 2015. These actions include moves to address delivering capabilities incrementally to meet warfighter needs vice waiting to deliver full capabilities in the outyears.

CHIPS asked Vice Admiral Brown to discuss the Joint Net-Centric Operations Campaign Plan and other ongoing initiatives in support of the joint warfighter in March 2007.

CHIPS: How does the plan help the joint warfighter in assisting the Iraqi government in stabilizing the population and in nation building?

Vice Adm. Brown: The plan is focused on delivering capabilities to improve warfighter effectiveness. The primary initiatives under way include operationalizing cyberspace; addressing information sharing issues; driving changes to coalition networks; and tackling the spectrum management challenges our warfighters face in ongoing operations.

First in operationalizing cyberspace, my staff is leading efforts to provide better information assurance capabilities to the combatant commands, establish quality training for our cyberspace professionals, conduct annual cyberspace war games (for example, Bulwark Defender), and develop innovative national and military policy in this critical warfighting area.

Second, through the plan, my staff is sponsoring information sharing initiatives in support of coalition and interagency operations. Teaming with the Office of the Assistant Secretary of Defense for Networks and Information Integration, we are developing a DoD information sharing strategy and associated implementation plans to facilitate improved communications between DoD elements and with our non-DoD mission partners.

Third, in direct support of the war on terror, we are driving changes to our coalition networks enabling significant improvements in our ability to share information with allies, mission partners, other agency partners and nongovernmental activities.

Finally, we are addressing numerous spectrum management initiatives critical to warfighter effectiveness. We lack a joint spectrum management tool to do real-time spectrum planning, and spectrum allocation and deconfliction on the battlefield, not only between U.S. forces, but with our coalition partners and host nation authorities. Therefore, we have focused our efforts on providing staff support to the U.S. Central Command (USCENTCOM) and to the Joint Improvised Explosive Device Defeat Organization to help defeat the improvised explosive device threat.

We are also overseeing the development of both a near-term tool to assist in countering the IED threat and a future spectrum management tool suite to manage the electromagnetic (EM) spectrum used by the Department in a net-centric environment. Our near-term tool, the Coalition Joint Spectrum Management Planning Tool (CJSMPT), will deliver an integrated EM spectrum management and near-real time mission planning tool to enable frequency managers to perform EM spectrum planning and deconfliction from tactical through combined and joint task force levels.

CJSMPT will transition to become the baseline of our future spectrum management tool suite, called the Global Electromagnetic Spectrum Information System (GEMSIS).

CHIPS: Is the CJSMPT new or does it replace something?

Vice Adm. Brown: CJSMPT was in response to a Joint Urgent Operation Needs Statement from the warfighters to address immediate EM spectrum concerns. It builds on the concept of current tools but adds key functions that our warfighters do not have today,

namely, advanced spectrum planning, real-time deconfliction and a visualization tool that provides a picture of actual spectrum use.

CJSMPT links to existing databases resulting in a more comprehensive spectrum knowledge repository establishing a common display warfighters can use in building their plan for spectrum allocation and use.

CHIPS: The associate director of the White House Office of Science and Technology, will be leading the U.S. delegation at the World Radiocommunications Conference in the fall to present both U.S. commercial and defense spectrum requirements. Has the Joint Staff already provided warfighter requirements?

Vice Adm. Brown: Yes, we have been involved in planning for WRC for about two years. We are engaged with other agencies ensuring warfighter requirements are represented in all formal U.S. positions. My staff is helping build the U.S. government position that becomes an input to the U.S. national position on a multitude of issues.

The U.S. government position incorporates inputs from government departments and agencies, while the national position also includes inputs from industry. My staff, along with the OSD staff, has been working in various governmental working groups and has presented a consolidated request articulating warfighter needs. In addition, we will have several DoD representatives in attendance supporting the delegation.

CHIPS: You were in Iraq in 2005 for an eight-month tour as the Deputy Chief of Staff for Communications and Information Systems for the Multinational Forces-Iraq working to establish an IT infrastructure. Has it been sustained?

Vice Adm. Brown: Unfortunately, the way we swap out forces, we tend to swap out everything. The Army calls it RIPTOA, which is Relief In-Place Transfer of Authority. The problem is — it really is ripping because they take everything out, and the new group brings everything with them. They build everything from the ground up every time. It has been difficult to establish an infrastructure that's enduring.

The USCENTCOM J6 has done a great job establishing policies and procedures and being ruthless in saying, 'That's not the way we are going to do it. We have an enduring infrastructure here. We have a set number of applications and systems that support the effort and when you come in, this is what you are going to use.' We are at a point now where we are starting to build on that, and this upcoming rotation is going to be much different than the rotations in the past.

CHIPS: Is the network you referred to earlier for coalition collaboration, CENTRIXS, or something else?

Vice Adm. Brown: We have about 17 different CENTRIXS networks. They are different because of the releasability of information and the different partners that are on the different versions.

Initially, we are talking about trying to collapse all of those into one network and to use rules-based software that would allow access and provide for the distribution of information. It would be based on identity and how the rules were established in the network that say what you can see and what you can't see.

Once we are able to collapse CENTRIXS, we hope we will be able to move all data presently residing on it into SIPRNET. The ultimate goal is to get to the point where we have one network with all the information stored in the same database, and it's tagged to the point where my identity allows me to go into that database and see only what I am authorized to see.

I say we can get there within the next few years.

CHIPS: Hasn't CENTRIXS improved over the years?

Vice Adm. Brown: CENTRIXS is not dynamic. It is not agile. It is not robust. If I want to add a new partner on CENTRIXS today, it's going to cost me, initially at least, a million and a half dollars, and it will take about six months to do the paperwork. CENTRIXS has improved, but it is still cumbersome. The CENTRIXS capability is the best we have today, but we need to do a lot better.

CHIPS: The plan discusses how DoD will transition from IPv4 to IPv6. Has progress been made in this area?

Vice Adm. Brown: Progress has been made in this area, although not substantive progress at the warfighter level. The Department laid out the key elements of its transition strategy including a requirement that procurements, acquisitions and developments be IPv6 capable, while continuing to be IPv4 capable — our current environment. To minimize costs, we are attempting to acquire IPv6 capabilities through scheduled technology refreshment activities.

My staff is supporting the development of the DoD IPv6 Integrated Implementation Schedule, which provides a consolidated schedule for major networks and programs that support combatant commanders, the Services and agencies.

We are also supporting the DoD IPv6 Master Test Plan which outlines a coordinated approach for DoD IPv6 testing. The test plan establishes the operational criteria that must be demonstrated during the transition to IPv6.

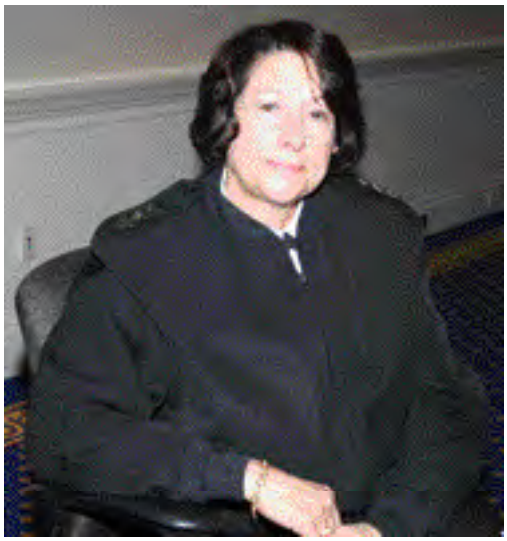
Finally, there are challenges we need to address in order to effectively transition to IPv6. First, we must ensure security is addressed before, during and after the transition. The development of IPv6 security tools must be accelerated. Second, the development of applications that showcase the benefits of IPv6 to the warfighter must also be accelerated. Third, we must address the perceived IPv6 performance degradation to ensure that as we transition, our investments are sound and will improve warfighter effectiveness.

As you can see, we are cautiously moving forward in this area.

CHIPS: Are you looking to industry to take the lead?

Vice Adm. Brown: Yes, we are looking to industry to share lessons learned and some of the issues they have tackled in transitioning to IPv6. The Defense Information Systems Agency has an IPv6 laboratory and project office. We are working closely with the Services and DISA to work through IPv6 issues and how we can mitigate them.

The transition from IPv4 to IPv6 must be seamless. We cannot afford to put at risk our current operational capabilities during this transition. We must maintain interoperability and security during and after the transition to IPv6 while continuing support for IPv4 legacy systems. We are also charged to provide the Chairman with a recommendation on the benefits and operational risks of going



Joint Staff Director for C4 Systems Vice Adm. Nancy Brown during the interview with CHIPS March 29, 2007. The admiral was in Virginia Beach, Va., for the day to participate in the Network Centric Operations Industry Consortium Plenary Meeting. The NCOIC mission is to facilitate global realization of the benefit inherent in net-centric operations.

to IPv6. Before DoD makes the leap, the Chairman has to certify that it's the right thing to do. We are working with DISA and the Services to mitigate risks and determine the key components of the Chairman's certification.

CHIPS: Will there be unique aspects to the application of IPv6?

Vice Adm. Brown: Yes, there are unique capabilities that IPv6 provides, such as expanded address space, enhanced quality of service, and expanded discovery of services, that will allow us to do more in a net-centric environment. However, before we declare victory, realize that IPv6 capabilities are in varying states of maturity in the areas of development, testing and delivery. We must have full situational awareness of enhancements in these areas in order for us to effectively collaborate with other federal agencies for the safe and economical adoption of this new technology. To fully leverage IPv6 capabilities, we must not lock ourselves into employing IPv6 in the same manner we employed IPv4.

Finally, we must take a long-term view to focus on what provides the greatest benefit to the warfighter and invest in proven capabilities that lay the foundation so that we can take advantage of capabilities as they evolve and mature.

CHIPS: Can you talk about the problems associated with maturing the Global Information Grid?

Vice Adm. Brown: The real challenge is to make the GIG relevant to the DoD information enterprise. We have to take on a data centric approach. The bottom line is: we have to get to the point where data is accessible to all users that require it, including unanticipated users. We will accomplish this through effective implementation of our data strategies and standards. When the enterprise gets this right, the communication infrastructure of the GIG can be resourced and maintained by the Services and DISA.

Another challenge to maturing the GIG is how to transition legacy equipment and applications to the GIG, while providing continued operations and maintenance of systems operational on the GIG. We are engaged with DISA to ensure joint warfighting capabilities are effectively incorporated into the Defense Information Systems Network, or DISN.

DISA is actively working with the Services and agencies to efficiently transition from legacy systems to emerging systems that facilitate joint network-centric operations. In addition, the Office of the Secretary of Defense, Program Analysis and Evaluation, is leading a working group to review the proposed investments for the DISN and to develop a way to finance the validated requirements.

The Joint Staff, various organizations within OSD, the Services and agencies are actively participating in this working group to identify what is required to sustain the network and meet the warfighter demands on the network as operations continue to become more net-centric.

CHIPS: What does "pervasive knowledge" mean in the plan?

Vice Adm. Brown: Pervasive knowledge is the result of effective knowledge sharing and can be described as the ability to permeate or spread information or thought throughout a group of individuals. Operating in a pervasive knowledge environment, users get information or knowledge at any place, at any time in the proper context.

Knowledge management is a mind-set enacted by people, enabled by process and enhanced by technology. Knowledge management processes help foster a culture of information sharing and help knowledge workers organize information and determine applicability to specific persons, organizations or processes. As derived from the NCOE JIC, knowledge management is the ability to systematically discover, select, organize, distill, share, develop and use information in a social domain context to improve warfighter effectiveness.

CHIPS: Can you give me an example of pervasive knowledge?

Vice Adm. Brown: Pervasive knowledge is having knowledge available wherever you are. My vision is that as a commander, I would walk into the command center and identify myself with either a fingerprint or my retina (whatever biometric is eventually chosen) but not a common access card, or something else I need to remember to take out of my wallet or switch out of my jeans to my suit. The source of my identification needs to be something that is with me all the time that identifies me dynamically and gives me the access I need wherever I am.

So I walk into the command center, and the command center is there to support the way I make decisions. I put in my fingerprint, I am recognized and automatically the screen and all the displays go to my personal requirements for the information I need in a way that I can synthesize it, and it allows me to make immediate decisions with the best quality information available — so that I can make sure that my force stays in front of the enemy in their decision process.

CHIPS: How far away are we from your vision?

Vice Adm. Brown: I think the technology is there to support at least 80 percent of the vision, but the culture is still a little bit farther away from being able to do so.

We have to get beyond the way we traditionally set up organizations and the way we structure information in an organization. We have to get to a point where it is not the J-2 who is holding all the Intel data and not sharing it, and the J-3 who has another set of data and the only way the commander gets an overall picture is

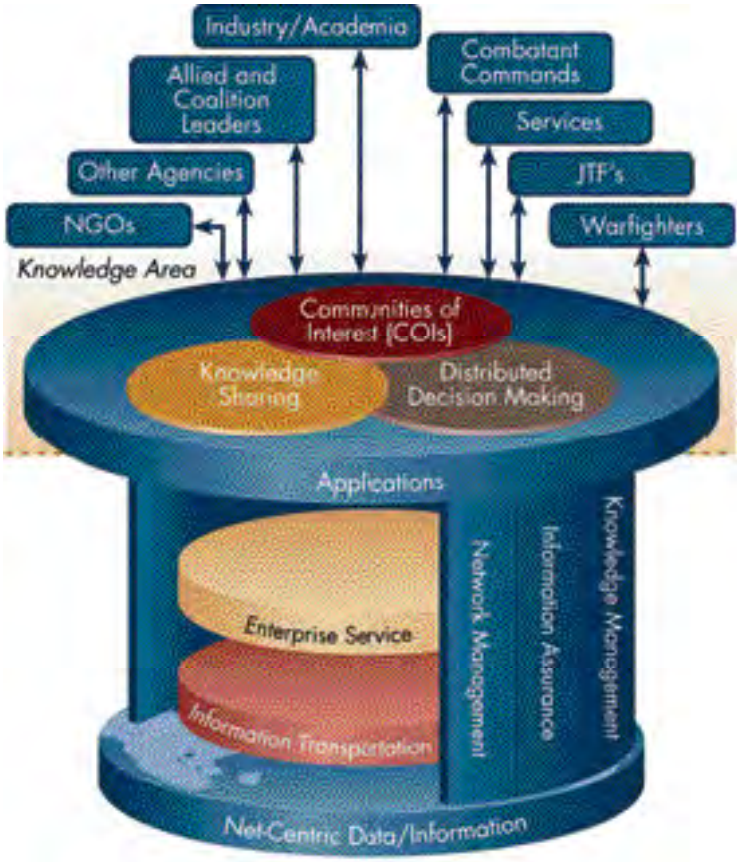


Figure 1. The Joint Net-Centric Operations Context as illustrated in the JNO Campaign Plan.

by taking what each one of the J-codes gives him or her and then synthesizing it themselves. *(An illustration of the JNO context of sharing knowledge and information in joint warfighting is shown in Figure 1. Figure 2, on the next page, shows JNO Observe-Orient-Decide-Act (OODA) Loop integration.)*

We must get to the point where an organization does not work in structured J-codes but in functional areas that synthesize the information and can put it all together — and when the commander needs it — it is decision-quality information.

CHIPS: The JNO calls for dynamically supported operations at every echelon, especially warfighters at the "first tactical mile." At that level of engagement how is the word getting out about what's available?

Vice Adm. Brown: Great question. I'll address it in two parts. To get the word to the warfighter, we need to ensure two things: processes are in place to ensure information can be appropriately discovered and that network connectivity exists so that the warfighter has timely access.

Historically, the communications and information community has not done a good job communicating how to access a wealth of information available to the warfighters via reach back or about our present efforts to move to a joint net-centric operational force. We have got to do a better job of demonstrating the operational relevancy and benefits of capabilities being delivered to the warfighters.

To get the word out, I recently published the J-6 Strategic Communications Plan – a tool to develop and communicate key messages throughout the Department, to industry, academia and any user or developer of joint net-centric capabilities for our warfighters.

We are working the gaps associated with delivering joint net-centric capabilities identified by the combatant commanders through their Integrated Priority Lists submissions and gaps identified through the JNO Joint Capabilities Document (JCD). Two of the net-centric 'Most Pressing Military Issues' are 'improve information sharing with mission partners' and 'improve information transport capabilities to enable joint forces in net-centric operations.' We are supporting efforts to the JROC to address these immediate warfighter needs.

The need to share information has been identified by seven of the nine combatant commanders. They require the ability to: share, collaborate and synchronize information with mission partners; extend sharing capabilities to mission partners; and provide exportable and affordable capabilities to less capable mission partners. The geographic combatant commanders continue to highlight the importance of this connectivity and are demanding further expansion of these capabilities.

The recent report of increases in hostile attempts to penetrate and disrupt our networks has highlighted the need for greater defense in depth and enterprise solutions to better protect sensitive information. The Enterprise Solutions Steering Group (ESSG), a joint forum with representatives from the Joint Staff, OSD, the Services, DISA, the National Security Agency and combatant commands, fields key information assurance tools that provide much needed computer network defense capabilities to the warfighter. In the past two years, the ESSG has fielded sensors, vulnerability assessment and remediation tools, antivirus/anti-spyware capabilities and host base security systems.

Another tool to address immediate warfighter needs is through the Command and Control Initiatives Program (C2IP). This program allows us to be more responsive to combatant commands emerging or emergency needs. I have some great people working on the answers to some of our most difficult problems. Solutions they recommend are often at the very cutting edge of technology or are so out of the box that an acquisition program to fund them in a three-year (normal) budgeting cycle just won't do.

Through C2IP, I'm able to put dollars where there are needs today for our warfighters to connect them. With our program, we are able to fund C2 solutions putting 21st century C2 solutions into Third World environments.

In addition, in remote locations in Central America where we daily fight the war on drugs and narco-terrorism, we've been able to fund programs to enable secure communications and reach back to forward deployed forces.

Finally, we were able to provide the Commander, Joint Task Force Horn of Africa (CJTF-HOA) with a Navy surface ship identification system – a program for Navy vessels to deconflict themselves from commercial traffic afloat. The CJTF-HOA J6 required this system to monitor ship traffic around the horn and through the choke point of the Strait of Hormuz.

This capability was critical to their ability to separate wheat from chaff as it pertains to drug, weapon and terrorist smuggling in and out of this troubled area. With minimal associated costs, we were able to meet the commander's needs in months versus years based on the traditional method for acquisition.

As you can see, we are using the campaign plan to address more than just doctrinal and training needs but operational and programmatic needs [as well] to deliver joint net-centric capabilities to meet warfighters needs.

Figure 2. JNO-OODA Loop Integration.

*Through JNO, warfighters will access secure information from both inside and outside their immediate environment and will **observe** real-time events and receive feedback from previous actions.*

*Through networking and synthesizing data from traditionally separate staff functions and collaborating with mission partners, warfighters will **orient** on the unfolding situation, as the network responds to their changing operational needs.*

*Due to the warfighter's access to information and knowledge, including the latest intelligence, surveillance and reconnaissance reports, the current operational picture and insights of subject matter experts and/or COIs, the warfighter will **decide** on appropriate courses of action and will **act** with improved effectiveness.*

CHIPS: Is it a decision-support mechanism at the first tactical mile?

Vice Adm. Brown: What I'm really talking about is that today we design a system looking at people sitting in a building on robust fiber — and not the folks that are on the tactical side that are fighting the war or conducting the mission. These folks are for the most part disadvantaged users because of limited bandwidth, and not carrying large computers with them; only PDAs or laptops.

Also, a major aspect that would improve first tactical mile information sharing is through more effective situational awareness (SA) using a common operational picture (COP). The COP provides joint and coalition forces a clear advantage over hostile forces by quickly delivering a more accurate SA picture to any warfighter. The ability to continue receiving relevant, prioritized information, even during degraded operations, is also a major capability that future systems must take into account. We have to design systems that provide them the capabilities they need.

We have to look at it from the disadvantaged user perspective and not with the user that has an OC-12, or an Optical Carrier with a speed of 622.08 megabits per second, at their disposal in a huge computing facility. We must look at the person on the ship, not the carrier but the small boy, and look at the Soldier on the ground in a tank, and what capabilities that we need to provide to them.

CHIPS: Who should be reading the campaign plan?

Vice Adm. Brown: It's our intention that every user and developer of C4 and joint net-centric capabilities read the Joint Net-Centric Operations Campaign Plan. We have made it available to industry, combatant commands, the Services, agencies and interagencies on our Web site.

From CIOs and action officers to noncommissioned officers, the plan serves as a valuable tool to shape their perspectives of the JNO vision. The plan establishes the unifying strategy to better integrate and synchronize joint community transformational efforts in order to maximize warfighting capabilities in a net-centric environment. It is being used to establish a common framework within DoD to help define and describe processes for combatant commands, the Services and agencies that participate in capabilities validation, resourcing and acquisition. The plan sets the foundation for where the joint community needs to progress over the next two to five years to deliver joint net-centric operations.

CHIPS: I understand that you are interested in feedback. I read the campaign plan, and it's fascinating. But if I am a project leader, it doesn't tell me what I need to do to fit into the joint strategy.

Vice Adm. Brown: The campaign plan itself, the document, is high level, and it talks about goals. But if you go to the Web site, the specific actions that we believe support attaining those goals are listed. It tells you what we are doing, or who else is working on it and where we are in completing that action.

I can understand the comment that the campaign plan doesn't tell you exactly what you need to know, but if you go to the Web site [http://www.jcs.mil/j6/c4campaignplan/Annex_A_JNO_CampaignPlanOct06.pdf], and look under the goals and action items, there are over 120 action items that support the campaign plan. For each action item there is a point of contact.

CHIPS: The plan calls for collaboration with coalition partners to promote combined interoperability through standard policies and procedures. How will this be accomplished?

Vice Adm. Brown: The J6 is the designated DoD lead in several international forums to work collaboration for policy development, procedures and standards. Through NATO forums, the Combined Communications-Electronics Board (CCEB) and the Multinational Interoperability Council (MIC), my staff is able to influence coalition adoption of common policies, procedures and standards, as well as to adopt their best practices and lessons learned.

Joint net-centric operations transcends international boundaries, and J6 continues to partner with our NATO allies to bolster JNO capabilities. We are heavily engaged in NATO's Network Enabled Capability (NNEC) development. NNEC supports NATO's three transformation goals: decision superiority, coherent effects and joint deployment and sustainment. NNEC enables NATO's ability to conduct net-centric operations and supports information sharing among the NATO nations.

For my part, it is encouraging to see that NATO views net-centric operations and information sharing as we do. The NNEC effort is a positive step forward for developing both a strategy and roadmap that will enhance multinational information sharing activities. Through our collaborative efforts via the NATO Consultation Command, and Control (C3) Board, we will continue to improve those vital capabilities for coalition warfighters current and future.

CHIPS: Do you have to wait for funding for the new network capabilities that are specified in the plan?

Vice Adm. Brown: Currently, the Department has a number of large, key net-centric programs already funded that start delivering in the 2012 to 2015 time frame. We are looking at things we can do today, in the next couple of years, which give us some of those capabilities faster and allow us to start transforming before the 2012 to 2015 timeframe. There are certain things that need to be in place before those programs start delivering, such as policies and tactics, techniques and procedures that support those programs and technologies.

One method we have used to influence future network capabilities is our active participation in the DoD CIO's GIG enterprise-wide systems engineering efforts. It is critical that we, as the warfighting domain, set the operational context and priorities that establish these forward looking standards and performance metrics.

We have also started laying the foundation for changing how we do things so we can take advantage of the technology when it starts being delivered. We are synchronizing programs to ensure that as capabilities are delivered warfighters can use them immediately. For example, we have synchronized our space programs so that when we launch a Wideband Global Satellite Communications (WGS) system or Transformation Satellite Communications System (TSAT), the ground infrastructure is in place, and the Services have the terminals to use it.

A satellite is a big investment — and if you launch a satellite with nobody having a terminal that can use the satellite capability — you may be wasting valuable resources. The Department can't afford to do that.

CHIPS: The plan calls for specific actions within a two to five year time span. How will you measure progress?

Vice Adm. Brown: We use the campaign plan objectives and actions to continuously measure ourselves against our goals. This iterative process forces us to reevaluate our plan against the Chairman's priorities as well as the feedback we receive from the theaters and CIOs across the Department.

We use the plan to engage with the combatant commander J6s to identify and address strategic C4 issues affecting their ability to meet mission needs. As recently as February of this year, we gathered in Europe, hosted by European Command, to aggressively assess where we are with current initiatives. As a result, 16 new actions were added to the ongoing efforts to cover capability gaps.

We also brief high interest issues in the plan to the DoD CIO and C4 principals to gain consensus or vector checks on the actions in progress. This gives senior CIO and C4 leadership a chance to impact what we are doing.

Finally, the plan is a living document. My action group is working to develop appropriate metrics to measure our effectiveness. As such, key objectives and goals are briefed weekly allowing me to intercede on actions not moving ahead or that need vectoring. Upon completion of that review, the updated status of actions is posted on the J-6 Web site (SIPRNET only) for all stakeholders to review and provide comments or feedback.

CHIPS: With all your years in joint assignments, are you still active in the Navy Information Professional community?

Vice Adm. Brown: I am the senior Navy IP and the community sponsor. I take that very seriously and spend as much time as I can working on community issues and promotion plans and the assignment slates — and keeping track of where our folks are. When I travel, everywhere I go, I try to do an IP session so I get to see as many of the IPs as I can.

CHIPS: How many are in the community now?

Vice Adm. Brown: There are about 519 in the community. If we add in the limited duty officers (642X) and the warrants (742X), you'd get about 800 officers.

CHIPS: From what we hear from the IP community, they really enjoy their jobs.

Vice Adm. Brown: I think they do. We are a high-demand, low-density community. We are very much in demand, and there are not enough of us to go around. We have really taken on the Individual Augmentee mission. We have over 50 full-time yearly Individual Augmentee requirements, billets, in Iraq, Afghanistan, Horn of Africa and Guantanamo Bay.

Community-wise, there is a much higher percentage of IPs on the ground fighting the war than most of the other communities. When you look at our total inventory, we are a small community that delivers great dividends for the Navy and the joint community.

CHIPS: Do you see the community growing?

Vice Adm. Brown: I think the community has to grow a little bit. We have to figure out what the Navy needs from an information-based community in 2012. Are there other communities doing similar things? We need to take a look at this spectrum of communities that work in the information domain, what their skill sets are and what we think the Navy is going to need in 2012 and look to see if we have the right community construct in order to support that future requirement for the Navy.

As we work through that, there will be changes in community structure and the numbers for IPs may change — we may not be IPs any more. We may be called something else, or we may take on some functions from other communities, or there may be some consolidations.

I think there will be some change; I am not sure what it will be. We have an Integrated Process Team supported by Naval Network Warfare Command that is the Information Warfare community, formerly known as cryptologists, the Intel community, the oceanographic community, or 'METOCs,' and the IPs to see where there is synergy and where the differences are so great that you would not want to combine.

The question we must answer is, 'What is the best construct to meet the Navy's requirements for information-capable warriors?'

Visit the Joint Staff J-6 on the Web at http://www.jcs.mil/j6/index.html. To view Vice Adm. Brown's biography, go to http://www.jcs.mil/bios/bio_brown.html. To access the Joint Net-Centric Operations Plan go to the Joint Staff J6 Web site at http://www.jcs.mil/j6/c4campaignplan/JNO_Campaign_Plan.pdf. CHIPS

MobileNet: a new way for Soldiers to communicate with family

By the SSC Charleston European Office

Engineers in the Space and Naval Warfare Systems Center (SSC) Charleston European Office jumped at the chance to give Soldiers a little normalcy by way of access to a mobile cybercafé to maintain vital communication links with family and friends and the *Stars and Stripes* e-newspaper. They did this by designing and building a prototype of an Internet café that is mobile and easy to deploy. They called it: MobileNet.

The idea was to create a cybercafé to support joint warfighters deployed to the most remote locations around the world. MobileNet offers the Internet, webcams and voice-over-IP telephones via satellite technology. Although there are many similar technologies available to deployed Soldiers, none have the portability and ease-of-use that MobileNet offers.

The name "MobileNet" derives from the need to make the integrated solution mobile and to have networking built into the container. The prototype was designed and built under the direction of Ken McCullough, who was the program manager of the Internet cafés deployed to the Balkans when the idea of MobileNet began to take form. (McCullough now works in the SSC Charleston Intelligence and Electronic Warfare Division.)

The European Office has a long history of communications projects for Morale, Welfare and Recreation (MWR) in support of the U.S. Army Europe (USAREUR) Deputy Chief of Staff - G1, and is currently managing projects throughout the European theater in support of MWR and the joint warfighter.

The prototype conception to completion occurred in less than six months. The original prototype is still in use and operating in Romania in support of U.S. troops stationed there.

The prototype was extensively field tested in Europe over the last several years in support of joint warfighter exercises in Bulgaria and Romania.

The first production-ready prototypes were completed in spring 2006, and are currently deployed to the Operation Iraqi Freedom and Operation Enduring Freedom theaters. The initial order for MobileNet units was four with two already in use and the remaining two en route to theater locations.

One of the main goals was to design this system with simplicity. Total integration and a complete package was a desired outcome for the customer, but also something that would require less technical support. That is why a fully automated satellite communications system was chosen.

MobileNet can be operated by anyone with general computer knowledge, thus reducing setup time and the need for expert satellite technicians on-site. Once the system is set in place and has power, the startup time is less than 15 minutes to bring up the capabilities of the entire cybercafé.

MobileNet can be built for about $330,000, which does not include monthly satellite time costs.

Future MobileNet projects will improve return on investment, customer expectations and available options to an already great track record of designing leading edge communication solutions — and it is another example of how SSC Charleston supports the joint warfighter. The MobileNet option gives customers the proper tools to support the global war on terror with communication packages that have little to no burden on the facilities or commanders wherever MobileNet is located. CHIPS

MobileNet fits easily into a 30'x8'x8'6" shipping container.

MobileNet Snapshot

- Equipment fits in a 30'x8'x8'6" shipping container
- Certified to transport via C-130, C-17 or C-5 aircraft
- Built-in transformer for U.S. or European power supply
- Environmental control is maintained by a two-ton HVAC unit
- 12 workstations with 12 VOIP telephones optional
- Floors are covered with Rhino Liner, which resists scuffs, stains and dirt
- Walls are entirely covered with white dry-erase material for notes
- Uninterruptible power supply (UPS) for control room equipment
- Server rack provides ample space for the UPS, satellite modem, satellite dish controller, router, laptop and *laser printer
- Chairs are traditional "bowling alley" chairs that are bolted down for stability and dual seating configuration
- Computers are stored in overhead bins to reduce dust and dirt and strengthen security
- Monitors use two USB ports for Soldiers to upload or download pictures to and from family members
- Lexan covers protect monitors and webcams
- Stainless steel kiosk keyboards that resist dust, dirt and liquid spills
- Gun racks

Optional equipment includes:

- Plasma television for Armed Forces Network (AFN) broadcast
- LCD television mounted at entry point for X-box or PlayStation gaming area
- Exterior design can include custom-made designs or logos at customer's request

The configuration of MobileNet can be modified to fit any customer's needs with minimal effort and design time. The current turnaround time for a unit to be delivered is 12 weeks.

**A laser printer for Stars and Stripes reduces MWR's shipping costs for hard copy distribution of the newspaper.*

Interview with Lt. Col. John A. Nagl
Commander, 1st Battalion, 34th Armor Regiment

Lt. Col. John A. Nagl speaking to a luncheon audience at West 2007.

Collaboration on Field Manual 3-24 - Counterinsurgency began in 2004. It had been 20 years since the Army published a formal field manual devoted to counterinsurgency operations, and 25 years since the Marine Corps published its last manual on the subject.

Because counterinsurgency is so complex encompassing a people's socio-economic make-up, culture and religious beliefs, the manual only establishes guidelines with historical lessons and insights.

Counterinsurgency is often described as a mix of offensive, defensive and stability operations. Thus, the demands on American and coalition troops are equally complicated. Now, they must be nation builders, facilitating the establishment of local governance and the rule of law. They must provide humanitarian assistance and build trust with the local population.

CHIPS asked Lt. Col. Nagl, who is a recognized authority on counterinsurgency and assisted in the development of the field manual, to talk about its importance to the global war on terror. Nagl was interviewed Feb. 2, 2007, after his luncheon remarks at West 2007, co-sponsored by AFCEA International and the U.S. Naval Institute.

Nagl is the author of *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*.

CHIPS: Because the enemy can adapt easily to changes in the field, isn't it dangerous to have the manual so openly available?

Lt. Col. Nagl: The principles of counterinsurgency are largely timeless and counterinsurgency is very different from the insurgency. Even if the insurgent knows what we are trying to do — and he does have our playbook— it doesn't enable him to defeat us. The important thing now is that for the first time we all have a playbook.

The decision was made way above my pay grade, that is was important to have this document readily available to all of us — Army, Navy, Air Force, Marines, CIA, State Department, United States Agency for International Development, or USAID, and our nongovernmental partners — to get all of us working off the same sheet of music. It is worth the risk of tipping our hand to the enemy.

A lot of the agencies and partners that we need to work with don't have security clearances, but they are engaged in the fight, and we need their help to win the war!

CHIPS: So U.S. allies and partners should also be reading the manual? Would it help the average American to understand the war on terror to read it also? Where can we find it?

Lt. Col. Nagl: The average American would absolutely benefit from reading this field manual. It helps to explain an important component of America's national strategy for winning the global war on terror, which my friend, David Kilcullen, a former Australian infantry commander, has described as a *Global Insurgency*.

The more American citizens and our global partners know about the kind of war we're fighting, and our strategy to win it, the more support we'll have for the Soldiers, Sailors, Airmen and Marines, diplomats, aid workers, and intelligence officers whose help we need to win it. The manual can be downloaded at http://www.leavenworth.army.mil.

CHIPS: Who are the authors of the field manual?

Lt. Col. Nagl: Army Lt. Gen. David Petraeus [the top U.S. commander in Iraq today] and Marine Corps Lt. Gen. James Mattis provided the leadership and the vision for the project, but the editor of the project was Dr. Conrad Crane. Crane is a retired Army lieutenant colonel with a Ph.D. from Stanford who was honored by *Newsweek* as a "Man to Watch" for his contribution to the intellectual development of the Army and Marine Corps.

'Con' pulled together a team of Army and Marine Corps veterans of the wars in Afghanistan and Iraq and a number of academics, most of whom were also combat veterans.

Although we did talk with people from all of the services, and we do have an 'Air Power in Counterinsurgency' annex, this is primarily a land forces document. The Department of Defense is working on a Joint Counterinsurgency Manual, while the State Department is taking the lead on a manual to help the rest of the government understand its critical role in counterinsurgency.

CHIPS: You talked about how we are not making enough use of information operations or IO. There are many different theories on how to proceed. One British analyst said it is important to engage the women in the population. He gave the example of how the women of Northern Ireland demanded a stop to the insurgency there. Are we engaging Iraqi women? Do we know what they are thinking?

Lt. Col. Nagl: It is an enormously difficult constituency to reach. The security situation in much of Iraq has made it even harder for women to express their opinions publicly. I don't know what opinions they are expressing privately. The power of that 50 percent of the population to effect change is immense. We need to mobilize the women for peace in Iraq.

We need different information strategies for the Kurdish Iraqis, for the Sunni Iraqis and the Shi'a Iraqis. We also need to further segment our message to have specific messages for the women and children in each of those segments of society. My sense is that we are not being as effective in information operations as we could be.

CHIPS: More and more Islamic women and children are being recruited into the insurgency.

Lt. Col. Nagl: The same is true in Afghanistan and throughout the globe. The key to success in the long war is empowering the majority of the Islamic people who want freedom and economic opportunity and human rights for all — both men and women. We have to think hard about how we achieve that objective as a nation, how we empower everyone to have that same sense of respect for human rights and opportunity for self-advancement and shared opportunity.

CHIPS: Because there is a need for nation building and humanitarian assistance, what kinds of organizations do you think need to be more involved in the war?

Lt. Col. Nagl: I think the State Department is absolutely essential in prosecuting the long war, but it does not have the same constituency that the armed forces do. The Department of Defense has done some neat things in terms of sharing money with the State Department to accomplish shared objectives. I would like to see many more Foreign Service Officers in Iraq to create true interagency teams at every level from districts through the national level.

The Provincial Reconstruction Teams that the State Department is standing up in Iraq and in Afghanistan are enormously powerful. We need more of those — and we need them to be more robust — but the State Department does not have the money. I would like to see more resources flow into the State Department to help prevent wars and also to enable us to better integrate all the elements of national power to win.

CHIPS: Is money the stumbling block or a matter of understanding what is needed?

Lt. Col. Nagl: It is fair to say that the State Department is not nearly as good at marketing themselves to the domestic audience as it needs to be. America loves its Soldiers, Sailors, Airmen and Marines, as well it should, but what September 11 demonstrated to us is that State Department officers and USAID officers are just as important in this war as the military is.

If America better understood the critical role [that] Foreign Service Officers are playing in Iraq and Afghanistan, we would have more of them. As an Army guy and a battalion commander, there is nothing I would like more than to have in my battalion, as it is getting ready to go to war, than a State Department officer under one arm, my USAID officer under the other — and my Central Intelligence Agency guy sitting across the table from me.

All of them can have reachback to their home agencies so that when we are deployed in Al Anbar Province I have my experts with me, but they also have all the resources of their agencies to call on. That is the direction I think we need to move toward as we create a truly unified U.S. government effort to win these very difficult kinds of wars [that] we are fighting.

CHIPS: You talked about the need to evaluate the different dimensions of the war, for example, the population's reaction to various events. U.S. Joint Forces Command has a modeling and simulation exercise called Urban Resolve that measures public attitudes, in addition to other factors. (See http://www.jfcom.mil/about/experiments/uresolve.htm.)

"The Marines and the Soldiers see the horrible conditions Iraqi young people are living under. They understand intellectually the desperation that is driving their actions. That does not necessarily help them at the point of impact. At the point of impact, the key is leadership."

Army Lt. Col. John Nagl in Iraq.

Lt. Col. Nagl: Having accurate measures of the depth of their anger would be enormously helpful in the operational design of the counterinsurgency campaign at every level from battalion through theater. If we could enable our commanders with that technology, with that resource, it would be enormously helpful.

CHIPS: And what to say to the population in case counterinsurgency efforts cause a disruption to vital community services?

Lt. Col. Nagl: The message that I decide to send in my sector may or may not be the right message to send to those people, but I don't have the polling expertise or the depth of cultural knowledge required to craft the message correctly. There are other agencies that could help me do that more effectively.

I would have liked to have their help in Al Anbar in 2004 — and it is going to be just as important in Al Anbar in 2007.

CHIPS: There is a great deal of pressure on our troops engaging with local children and teenagers. They could be having a great time — handing out toys and playing games — and then go around the corner and those same children are setting off a bomb. Does the field manual provide any guidance in helping troops deal with these situations?

Lt. Col. Nagl: There is a whole chapter in the field manual, called 'Leadership and Ethics in Counterinsurgency,' on just that problem. The Soldiers, Sailors, Airmen and Marines have to understand the nature of the war we are fighting and also understand the drivers of behavior in the population. Unemployment in Al Anbar approaches 80 percent, and if I were forced to choose between my family starving to death, or setting an improvised explosive device for money to buy food, I would set an IED. I would take care of my family. That basic loyalty would come first.

We have to provide more economic opportunities for the insurgents, particularly for the Sunni insurgents. We also have to develop a political solution and information operations campaign — not to show them the error of their ways as much as to show them the brighter future — if they choose a different path — and if they come onboard with the economic development programs that we're working to develop in Iraq.

"Where I think we really need to work … is on the unblinking eye, persistent intelligence, surveillance and reconnaissance. There is more we can do … to provide a comprehensive picture of who the enemy is."

The Marines and the Soldiers see the horrible conditions Iraqi young people are living under. They understand intellectually the desperation that is driving their actions. That does not necessarily help them at the point of impact. At the point of impact, the key is leadership.

Our sergeants and our young officers are providing that leadership every day, 99.9999 percent of the time. It is a huge challenge.

CHIPS: What are some of the technologies that troops need at the ground level?

Lt. Col. Nagl: We are actually doing a remarkable job at the ground level. The body armor we wear, although it is heavy, is remarkably effective. I have Soldiers who absolutely 'ate' 7.62 mm sniper rounds in the chestplate and walked away. The individual Soldier gear is phenomenally effective. It can always be lighter. It can always be cooler. I know industry is working on those efforts.

Where I think we really need to work, and I am not a technologist, is on the unblinking eye, persistent intelligence, surveillance and reconnaissance. There is more we can do there and with the integration of various databases to provide a comprehensive picture of who the enemy is. The hard part in this kind of war is not killing your enemy; it is finding your enemy. There is more that technology can do to help us.

CHIPS: Are you talking about being able to see through buildings?

Lt. Col. Nagl: Looking through buildings would be great and listening to communications of various forms, and patrolling the streets with remotely-piloted vehicles and satellites. The hard part is how to integrate all of those disparate pieces of information together, and coordinate and tie them in with the human intelligence reports I am getting from guys I have detained and from man-on-the-street interviews.

To pull all that together to create one picture of who my enemy is, in my eyes, is the biggest problem fighting insurgency at the tactical level. There is more industry could do to help us pull all those pieces together and create a comprehensive picture: This is the bad guy. This is where he lives, and these are his friends. By the way, they never sleep in the same place twice, but on Wednesday nights, this is where they are likely to be at a 70 percent probability rate. Here is the picture of the house — and here are the satellite coordinates — and we've got eyes on him.

You then have: This is where you need to go. This is the guy you need to get. Here are his pictures. Here are his fingerprints. Here's what his voice sounds like, and here's the legal packet that is going to put him away for 40 years for killing American Soldiers. That's what I need.

Right now I am doing all of that myself with my brain power. Anything that industry can do to take some of the load off the overtaxed brains of our ground force commanders would be enormously useful.

CHIPS: I know the operations tempo is incredible, and the stress on troops is enormous. I have read in the media that there are cases where our troops are malnourished.

Lt. Col. Nagl: Absolutely not true. The average Soldier in Iraq gains 22 pounds in a year. They come back chubby. The first year in Iraq, 2003-2004, when I was there, the average Soldier did lose 10 pounds. We have now established a mature theater, and the big question is: 'Which flavor of Baskin-Robbins do you want?'

My baby brother is a buck sergeant in the Army in a remote area so he doesn't get all 31 flavors. I think he only has 12. He is coming back chubby as well, so I am going to have to run him into the ground to get him slimmed down.

"The hard part in this kind of war is not killing your enemy; it is finding your enemy. There is more that technology can do to help us."

No Army and no Marine Corps in history has ever been as well supplied as our Soldiers are in Iraq and Afghanistan. They have never had the instantaneous communication with home that they do today. Industry and our government have done an extraordinary job of supporting our Soldiers, Sailors, Airmen and Marines, and anyone that you talk to will back that up. I will strenuously defend our logistics.

CHIPS: How is equipment holding up?

Lt. Col. Nagl: We are working it hard. Tanks programmed for 800 miles a year are running 4,000. We are putting a heavy burden on our equipment and fixing it is going to take years after this war is over. We'll need the support of the American people to pay those bills to bring us back up to tip-top fighting shape when the fighting is done.

CHIPS: Anything else you would like to say to our readers?

Lt. Col. Nagl: Our Soldiers, Sailors, Airmen and Marines — and our Foreign Service Officers, CIA agents and USAID workers — are doing phenomenal work in the effort to bring lasting peace and security to the people of Iraq and Afghanistan. They deserve our continued support and our sincere respect.

Stability in Iraq and Afghanistan is essential to our safety here at home, and we owe our profound thanks to all of the Americans who are helping our Afghan and Iraqi allies confront horrible enemies who will stop at nothing to bring destruction and tyranny to those troubled lands.

For a copy of Field Manual 3-24 - Counterinsurgency, go to http://www.leavenworth.army.mil. Visit the 1st Battalion, 34th Armor Regiment at http://www.riley.army.mil/Units/1BCT1ID/1-34AR.asp. CHIPS

Q&A with Cmdr. Tony Parrillo

Director of the FORCEnet Execution Center and Trident Warrior Naval Network Warfare Command

Trident Warrior is the primary FORCEnet Sea Trial series of experiments sponsored by the Naval Network Warfare Command (NETWARCOM) and the Space and Naval Warfare Systems Command (SPAWAR). TW07, the fifth in the series, was conducted March 20 through 30 off the Virginia coast.

CHIPS spoke with Cmdr. Parrillo during Trident Warrior 2007 execution in March.

Trident Warrior director Cmdr. Tony Parrillo with Brad Poeltler, TW deputy director, at the TW07 Process Engineering Workshop in March. Parrillo received a 2007 Copernicus Award in February given by AFCEA International and the U.S. Naval Institute for his outstanding work in Trident Warrior.

CHIPS: What is Trident Warrior?

Cmdr. Parrillo: Trident Warrior is the major annual FORCEnet Sea Trial experiment. It's an experiment and not an exercise. TW03 was the first one. We have been gathering speed and capability over the years.

Within the experiment we look at an experimental environment like you remember from your high school chemistry days. Using controls and variables, we try to reduce the number of variables and have the greatest number of controls so that we know that we are getting the correct data that we need.

We also try to develop 'speed to capability' or rapid fielding. We have had great success getting information technology, which is the most rapidly changing field in the world, out to the fleet to make the Navy more capable.

We develop military utility recommendations. Obviously, the things we experiment with have military utility. If it does not have military utility then we really shouldn't be working with it. And of course, we want to impact the Navy budget and make sure the Navy is spending money on the right capabilities for the right price.

CHIPS: Why experiment, isn't it expensive?

Cmdr. Parrillo: Experiments actually drive down costs. We have these experimental venues which allow us to get the interaction of our Sailors on the deck plates using the technology rather than having guys in lab coats that may or may not have ever been in the military trying to guess what we need.

We get the technologies out early in the development process so that our Sailors can use them, and we can get the best recommendation, the best feedback, of what we really need. It helps us procure only what we need, and it helps us be good stewards of taxpayer dollars.

Since it is an experiment and not an exercise, we don't train the crews. We use new equipment that they just trained on, and they give us recommendations.

The good thing that we are also able to do is: We don't have to follow existing doctrine. We can try out a different doctrine and make recommendations to change the way the military operates.

Here are some of the military capabilities we are testing – maritime domain awareness is important with piracy around the world. You want free commerce because the better that goods travel across the ocean — the cheaper things are for all of us. Within that scope we have a lot of law enforcement focus.

The war on terror is not about 'bombs on targets' anymore; it's about arresting criminals and putting them behind bars for the rest of their lives. To further the CNOs' vision for the 1,000-ship Navy, we are actually working with coalition partners, which includes France this year. We have a great relationship with all those countries: Canada, Australia, New Zealand, Italy and the United Kingdom.

We will work on defense support for civil authorities — the state and local first responders. This part grew out of the Hurricane Katrina and Rita relief efforts. In addition, we are looking at humanitarian assistance disaster relief from the tsunami and the Indonesian earthquakes and assorted other crises around the world that the military has been responding to.

Department of Defense policies have changed; laws have been changed so that the military can provide greater aid, and we can leave our equipment behind when we are done after these humanitarian relief efforts.

There are traditional military items we are working on like the net-centric operations that allow the commander to react quicker and to have better information in his decision process.

There are around 80 technologies. It changes every day. Some days the functionality does not work. We have about 200 objectives. Trident Warrior is about the people, the process and the technology. We don't just concentrate on computers and machines. We worry about the commander and his subordinates and how the process is interactive.

Some of our players this year are: U.S. Joint Forces Command, Second Fleet, Royal Navy Commodore Steve Cleary working with Second Fleet as the Combined Forces Maritime Component Commander, the Harry S. Truman Strike Group, Carrier Air Wing Three and Destroyer Squadron Two Six. The Defense Department's experimental ship, the Stiletto is also joining us.

Other ships include the USS Hue City, USS San Jacinto, USS Oscar Austin, USS Annapolis; from Australia, the HMCS Charlottetown, HMAS Perth and HMAS Arunta; from New Zealand, the HMNZS Te Kaha; and from France, the FNS Lafayette.

We have a lot of players and folks working on shore. This isn't just military focused. The Virginia Beach Emergency Operations Center and a lot of other first responders including the Naval Criminal Investigative Service and the FBI are involved.

CHIPS: Can you talk about any early successes or disappointments?

Cmdr. Parrillo: The biggest successes of the last three years have been Subnet Relay and high frequency (HF) IP. Both are the transfer of Internet Protocol data over existing line-of-sight radio links. SNR uses UHF radio, and HF IP uses standard HR radios.

These systems were actually proposed by our coalition partners in TW05 for their low cost and widespread availability. They were such a success [that] they were proposed to become a program of record, and now we are fielding them as part of a Rapid Technology Transition to the fleet.

Other notable successes have been the acceleration of Automated Digital Network System (ADNS) Increment II by two years; the creation and expansion of the Coalition Maritime Forces Pacific CENTRIXS [Combined Enterprise Regional Information Exchange System] community of interest; and the acceleration of fielding of AIS Phase IIB and developing TTPs for the 'Defense Support to Civil Authorities' objective, just to name a few.

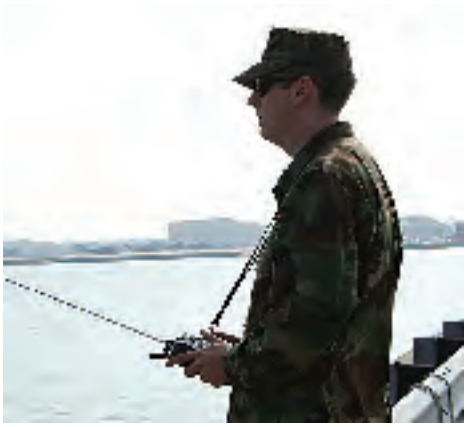
With ADNS Increment II, the Navy's family of shipboard routers will have dynamic bandwidth capabilities for better management. In the past the bandwidth for systems was 'locked in' — meaning so much of the ship's bandwidth was locked in for secret traffic and so much for unclassified traffic.

If the secret portion wasn't being used, it was wasted. Now if the secret side isn't being fully utilized, the unclassified side can use the bandwidth. The same with the phone lines, as soon as a phone is hung up, that bandwidth can be used for data.

AIS, the Automated Digital Network System, is the International Maritime Organization standard for ships at 300 gross or above. AIS Phase IIB is the latest Navy version to help bring this information into the Navy's common operational picture for command and control. Phase IIB brings added sources and functionality greatly increasing capability for the commander.

For disappointments, I won't name any specifics, but several large programs of record had missteps in performance that did not match design objectives. The good news is they were able to utilize the data collected and findings to redesign and improve their products. CHIPS

Top – participants of TW07 and members of the AUSCANNZUKUS TW07 team assemble on Naval Station Norfolk, bottom row: Canadian Navy Lt. Cmdr. Mike Turpin, Royal Australian Navy Lt. Cmdr. Kim Fisher, Canadian Navy Lt. Cmdr. Rob Sibbald and Royal Australian Navy Lt. Cmdr. Brian Cummins; middle row: Royal New Zealand Navy Lt. Cmdr. Danny Kaye, Canadian Navy Lt. Cmdr. Don Allan, Mr. Van Vu from the Australian Navy, Royal Australian Navy Warrant Officer Andy Kirkpatrick and Martin Jordan from SPAWAR; top row: Royal New Zealand Navy Lt. Jonathan Stirling, Mr. Max Lanchbury from the British Royal Navy, Mr. Paul Garnham from the Royal New Zealand Navy, Mr. Mark Coombs from the Royal Australian Navy and Mr. Steve Finch from the British Royal Navy.



OS2 Patrick Dow from the Navy Coastal Warfare Unmanned Vehicle Squadron communicating with the rigid-hull inflatable boat shown above during TW07 experimentation aboard Naval Station Norfolk. The white shield on the RHIB is a radiation detector. In actual operations the RHIB would be unmanned and sent out on security patrols guarding Navy ships against civilian boat traffic. Participants from NETWARCOM, SPAWAR, DoD, the Defense Threat Reduction Agency (DTRA) and industry staged an impressive demonstration of the technologies used in TW07 in March.

Defense Support for Civil Authorities ... a Vital Part of TW07

By Kevin Kurtz, Dan Dunaway and Brad Poeltler

Maritime domain security is a local, national and international concern and responsibility. To meet the challenges of protecting this complex environment, an assembly of representatives from multiple agencies including local, state, federal and international organizations met January 17 and 18 at the Tidewater Node of the FORCEnet Composeable Environment on Naval Station Norfolk, as the Trident Warrior 07 Process Engineering Workshop.

The purpose of the workshop was to evaluate and document detailed responsibilities and procedures in response to several potential maritime threats in the Hampton Roads area. Such procedures are vital to maximize awareness, define resources, and coordinate an integrated defense among a diverse group of response partners from the U.S. departments of Defense, Justice and Homeland Security, state and local law enforcement officials, and fire and rescue teams.

Though this may seem like an internal problem, U.S. partner nations are significant participants in situations that involve defense of the homeland.

Maritime Security

President Bush has underscored the importance of securing the maritime domain, defined as *"all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."*

This mandate requires the establishment of an integrated network of national-level maritime command centers to achieve coordinated, unified, timely, and effective planning and execution by the U.S. government in the event of a threat.

The president's guidance directs clear relationships and operational coordination among maritime domain agencies, enabling the U.S. government to act quickly and decisively. A federal Maritime Operational Threat Response Plan was developed that sets forth high level guidance for interagency coordination and assessment.

But for any operation to be successful, lower-level procedures must be established. Understanding interagency relationships and processes to integrate Navy command and control systems into the plan is the focus of the Defense Support to Civil Authority and Maritime Domain Awareness initiatives of TW07.

Experimentation

The Trident Warrior experimentation series is the primary FORCEnet Sea Trial exercise, conducted annually, and co-sponsored by the Naval Network Warfare Command (NETWARCOM) and Space and Naval Warfare Systems Command (SPAWAR). The experiments are targeted for "speed to market" to meet fleet requirements. TW07, the fifth in this series, was conducted in late March 2007 in the Norfolk, Va., area.

TW exploits advanced technology concepts to provide the warfighter with information superiority over an adversary to give him predominant decision-making ability for operational success in the battlespace.

One of the major experimentation areas is maritime domain awareness, specifically "Defense Support to Civil Authority." The workshop's goal was to document and measure development with a focus on information exchange requirements and methodologies. Action centered around four scenarios that required each participating agency to conduct a function of command and control.

The scenarios provided context to experimentation events: (1) a high value asset escort from sea to port, using liquid propane in this experiment as the HVA; (2) port of Norfolk security with a focus on the Norfolk International Terminal and Norfolk Naval Station, and a corresponding event with cargo transition to intermodal transportation; (3) a threat to the Chesapeake Bay Bridge Tunnel; and (4) escort of the USS Harry S. Truman (CVN 75) Strike Group from port to sea with a follow-on incident at the Chesapeake Bay Bridge Tunnel requiring interagency response.

Each activity was sequenced into a step-by-step evolution. The results were documented in several time-sequence diagrams to provide the procedural backbone to any comparable real-world operation. These procedures were executed with real forces during the actual TW experiment in March. Rigorous evaluation methods for the experiments is one of the hallmarks of Trident Warrior's success, according to the TW team.

"It is imperative that we enter into Trident Warrior 07 with

Participants in the Trident Warrior 07 Process Engineering Workshop gather in the SSC Charleston Tidewater Node of the FORCEnet Composeable Environment on Naval Station Norfolk in January 2007.

Other participants in the workshop and Trident Warrior execution, included coalition partners and a diverse group of first-responder partners from the U.S. departments of Defense, Justice and Homeland Security, state and local law enforcement officials, and fire and rescue teams.

"There is a lot of talk about sharing data and information between civilian and military authorities, but we are actually exchanging data and showing the value of collaborating in a common environment at both the operational and tactical levels of command."

– Kevin Kurtz

a solid baseline process in the context of the supporting scenarios, so that we have a framework to measure information flow and Trident Warrior technology or process treatments, and identify command and control system gaps for the responding community of interest," said Dan Dunaway, the TW07 lead for process development.

Data Sharing for Interoperability

Technical focus is on data sharing and interoperability. Unified procedures are vital, but it is equally important to have the major data providers and consumers available to make sure that methods for pulling and pushing data are accurately depicted in the process models. TW07 will continue development for an unclassified Crisis Preparedness and Response Network. The genesis of this network came from Hurricanes Katrina and Rita lessons learned.

The development team included NETWARCOM, U.S. Joint Forces Command, U.S. Northern Command (USNORTHCOM) and the Naval Surface Warfare Center Mission Assurance Division in Dahlgren, Va. The network has a collaborative common operational picture that includes static infrastructure data, dynamic Automatic Identification System tracks from USNORTHCOM, real-time weather conditions from the National Oceanic and Atmospheric Administration, imagery from the National Geospatial-Intelligence Agency and Federal Emergency Management Agency flood plains, as well as data from other sources.

According to the TW team, the actual importance of the collaboration wasn't the resulting map, as much as it was the sharing of data and understanding between the Defense Department and state and local first responders.

"There is a lot of talk about sharing data and information between civilian and military authorities, but we are actually exchanging data and showing the value of collaborating in a common environment at both the operational and tactical levels of command," said Kevin Kurtz, TW07 maritime domain awareness technical lead.

The procedural and technical recommendations from this workshop and Trident Warrior 07 will be incorporated into the procedures of all the participating agencies and organizations in the event of a real threat in the maritime domain.

– Kevin Kurtz is a retired Navy lieutenant commander and the maritime domain awareness technical lead for Trident Warrior.

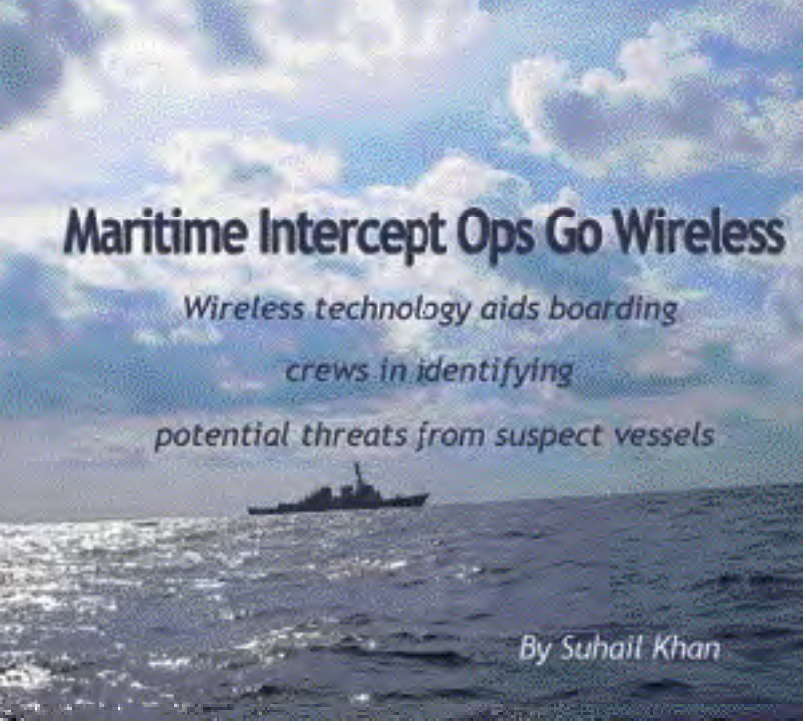
– Dan Dunaway is a retired Navy commander and the maritime domain awareness cognitive lead for Trident Warrior.

– Brad Poeltler is a retired Navy captain and the deputy director for Trident Warrior. CHIPS

Stiletto, the Defense Department's experimental 80 by 40-foot craft, took part in Trident Warrior 2007. Shown here aboard Naval Station Norfolk in March in communication with a rigid-hull inflatable boat.

Stiletto's commander and project manager, Cmdr. Jim Hruska, and Frank Wakeham, contract compliance manager for experimentation from the Naval Surface Warfare Center, Carderock Division aboard Naval Station Norfolk.

Space and Naval Warfare Systems Center (SSC) Charleston wireless network engineers, Glen Hoffman and Andrew Tash (right), explain the wireless networks tested in Trident Warrior aboard Naval Station Norfolk.



USS Carney (DDG 64)

On March 21, 2006, the Office of Naval Research approved a Rapid Technology Transition proposal from program office PMW 160 for an 18-month acceleration of a new capability for a wireless link between DDG-51 Arleigh Burke-class guided missile destroyers and target vessels in support of expanded maritime intercept operations (EMIO).

EMIO is a key maritime component needed to support the global war on terrorism by deterring, delaying and disrupting the movement of terrorists and terrorist-related materials and personnel at sea.

PMW 160, under Program Executive Office for Command, Control, Communications, Computers and Intelligence (C4I), developed a system that provides an 802.11g wireless link between the interdicted vessel and the host Navy ship up to two nautical miles away. The link transmits biometric data collected from the crew of the interdicted vessel. The data assist the ship's visit, board, search and seizure (VBSS) teams in identifying potential threats.

Because of the fleet's urgent need, Naval Network Warfare Command (NETWARCOM) funded an interim solution to provide wireless reachback functionality sooner. Recent attention gained by the project resulted in the Office of the Chief of Naval Operations taking keen interest in funding and immediate deployment of the interim solution for use in the war on terrorism.

From Dec. 4 through Dec. 8, 2006, Space and Naval Warfare Systems Center (SSC) Charleston personnel conducted security and operational tests at sea aboard the guided missile destroyer USS Carney (DDG 64). The five-day underway period for conducting mission preparedness exercises offered an opportunity for us to get aboard the Carney and demonstrate the tactical advantages of the system.

We departed Mayport, Fla., early morning Dec. 4 to conduct the tests. For the operational test, a rigid-hull inflatable boat (RHIB) posed as the interdicted vessel. As part of the tests, four distances ranging from 500 to 1,800 yards were tested. Biometric files were transferred from the RHIB to the host ship in less than three seconds with no errors.

During the test, USS Carney Commanding Officer Cmdr. Patrick Shea asked for a picture of the ship (shown at left) to be taken from the RHIB and sent back through the wireless link. Upon receiving the picture at the MIO platform through the wireless link, Shea sent the photo to his squadron, Destroyer Squadron 24, via e-mail as an example of the capability of the wireless link.

All tests were performed successfully by the SSC Charleston team with no detected vulnerabilities. Shea and the MIO boarding team were highly impressed by the tests and a positive naval message was sent by DESRON 24.

The system was tested again in Trident Warrior 2007, the premier FORCEnet Sea Trial series of experiments, in March. Look for more information about the results of the experiments regarding this new capability in the next edition of CHIPS.

Suhail Khan is a project engineer working in SSC Charleston's Communication Systems Department.

CHIPS

Suhail Khan mans a laptop in the background as USS Carney Commanding Officer Cmdr. Patrick Shea is all smiles after receiving a photo via the wireless link. The wireless link between the interdicted vessel and the host Navy ship reaches up to two nautical miles.

A team aboard the RHIB transfers files to USS Carney during recent tests for a wireless link in support of maritime intercept operations.

Interview with Royal Navy Commodore Steve Cleary Deputy Director, Combined Joint Operations from the Sea Center of Excellence


Royal Navy Commodore Steve Cleary

As military forces around the world transform the way they organize, plan, train and fight, Commander, U.S. Second Fleet has established the Combined Joint Operations from the Sea Center of Excellence (CJOS COE) to provide Joint Maritime Operations expertise for partner nations by drawing from more than 50 years of expertise as Commander, NATO Striking Fleet Atlantic. The CJOS COE functions through close liaison and cooperation with Allied Command Transformation, other maritime COEs, NATO joint force commands and numerous national commands.

Royal Navy Commodore Steve Cleary, deputy director of the CJOS COE, talked to CHIPS about 2nd Fleet's role as the Combined Forces Maritime Component Commander in the Trident Warrior 2007 series of experiments conducted March 20-30 off the Virginia coast. Trident Warrior is the primary FORCEnet Sea Trial exercise sponsored by the Naval Network Warfare Command (NETWARCOM) and the Space and Naval Warfare Systems Command (SPAWAR).

CDRE Cleary: We are trying to exploit advanced technologies and technology concepts, which hopefully will provide people like me, the warfighters, with information superiority, which means we will be better than our adversaries in the maritime environment. Superior decision-making capability is the entire aim of warfare at the operational level.

CHIPS: What do you hope to achieve for the coalition?

CDRE Cleary: The allies that will be participating in Trident Warrior are: the Canadians from their Regional Joint Operations Center in Halifax, Canada; the 'Brits' in London at Northwood Maritime Fleet Operations Headquarters; NATO at their Maritime Ops Centers in both Northwood and Naples; and America, from the U.S. Joint Forces Command, Joint Experimentation Center in Suffolk, Va., U.S. Sixth Fleet in Naples, U.S. Second Fleet in Norfolk, and the USS Harry S. Truman Strike Group participating at sea.

It is not the biggest coalition of NATO participants, but it is a start, and you have to start somewhere.

I am hoping to achieve a common set of processes and procedures so we can then spread that out further within NATO and further out of NATO. You don't have to be a member of NATO, and it can't be just members of NATO participating in what we are trying to achieve through this — which is maritime situational awareness. It used to be called maritime domain awareness, but the preferred title now — in NATO language — is maritime situational awareness.

If we do get common processes and procedures through the Maritime Headquarters/Maritime Operations Centers, or HQ/MOCs, in America, Canada, Great Britain and NATO proper, we can then force and push that throughout the 26 nations that make up NATO. And then go beyond that. This is a global issue. The sea encompasses so much of our workspace, our environment, that we have got to control it. We have got to control it better than we may have done in the past.

We are very good at maritime military operations in a wartime environment, like the Falkland Islands conflict in 1982 and the first Gulf conflict in 1991. It is that stuff that goes on outside of the military fighting operation that we need to be better at, [and] that's measuring our maritime environment for those vessels coming out of, for example, the Strait of Gibraltar, the Malaccan Straits or whatever. They've come from somewhere and they are going somewhere. As long as they are going about their business in a normal, decent, peaceful fashion there should be no concern whatsoever. But we know that there are vessels out there carrying bad people, bad equipment and weapons of mass destruction, illegal drugs, and illegal this or that. Those are the people we need to identify and measure and monitor.

That is what we are trying to improve with this MOC headquarters around as much of the world as we can to be better at maritime situational awareness in the maritime environment.

CHIPS: The British have longstanding experience in port safety and maritime dominance. Are you bringing that experience into Trident Warrior even though no British ships are participating?

CDRE Cleary: We will. It is very kind of you to say that we have a lot of experience. I think that we have. That doesn't necessarily mean that we don't still have a great deal to learn. The enemy continues to evolve and adapt. We must continually evolve ourselves to outpace them. We must ensure freedom on the seas and littorals, while denying the enemy the same. We must lean on our collective depth of experience, both successes and failures, but we must embrace innovation as well.

When were we good? Were we good at the Battle of Trafalgar when we came across the combined French and Spanish? Yes, we were. Are we good at the moment at maritime situational awareness? That's a new environment. We are now in a terrorist environment through asymmetric warfare, and we are not sure what's going on. We face challenges never before imagined. We need to be better at that, and I think we are getting better at it.

Today's maritime threats are elusive — enjoying sanctuary in their globalized, non-nation state existence. Traditional sorts of sea power such as 'gunboat' diplomacy and deterrence have little effect. Our only hope is for ourselves to coordinate globally.

A problem from Naples is not just a threat to Italy. A problem from Toulon is not just a threat to France. Today, there is simply no such thing as a regional threat — all threats are in some way global. The more we link into other people, often people we traditionally would not have linked into, the better we will be able

to identify such threats, understand their intent, and then determine how to respond.

If a threat comes out of the Atlantic and then goes through the Strait of Gibraltar, and it is somebody we have absolutely identified as a critical contact of interest for whatever reason, we need to make sure that information is passed into the Mediterranean. Then we go back to that process of what we do about it. Tail it? Monitor and board? Apprehend?

The processes we have to work out — and soon — go beyond information sharing. These are the processes and procedures that we have to establish. If it [a threat] pops up in your area, what do you do? If it pops up 300 miles off the East Coast of America, what do we do?

CHIPS: Is there any one technology or phase of the experiments that you are particularly interested in?

CDRE Cleary: It is mainly the common processes. We are using a number of technologies for passing information, such as BRITE, NATO's developing collaborative capability for maritime operations, awareness and information sharing. There are a number of other technological solutions we are experimenting with throughout NETWARCOM and SPAWAR.

There are about 200 objectives out of about 80 technology experiments overall in this experimental exercise that we are trying to achieve. Mine is only one part of it. There are numerous other experiments delivering objectives that are being worked here. There is an awful lot going on.

Here in NETWARCOM and SPAWAR, people like Brad Poeltler [TW07 deputy director] are working it everyday — all sorts of technological solutions to improve and give people like me, the warfighting person at sea, decision superiority over our adversaries. That is the whole aim of this business.

CHIPS: How would local and regional law enforcement and other agency people respond and share information with the Navy?

CDRE Cleary: That is a good point. I remember through Hurricane Katrina some well-advertised shortcomings that came across during the hurricane: federal, state and the local coordination and maritime and land coordination. It is not just about maritime on maritime or maritime with air support and maritime with land — it's about interagency business. This stuff that is at sea has come from land somewhere, and this stuff that is at sea is going to land somewhere.

We can only do so much — and if we don't have that interagency linkage set up — we will fail. It will get so far — and then it will stop — and we will lose it. If it comes close to the U.S. Eastern Seaboard, the U.S. Coast Guard will have responsibility.

It couldn't be more true, when you mentioned that bit about the interagency and coordination. I have seen it go not so well. I believe there were some coordination issues that came out in Hurricane Katrina that we need to be better at. That is not a criticism of this country but an observation from my participation in Katrina.

I don't know if you intend involving yourselves during Trident Warrior itself. If you do, I'll be in Suffolk at the Joint Warfare Center throughout the entire period at the U.S. Joint Forces headquarters. This is another example of interagency cooperation.

Royal Navy Commodore Steve Cleary, deputy director of the Combined Joint Operations from the Sea Center of Excellence, talks to members of the media about the importance of Trident Warrior to coalition partners just before Trident Warrior execution March 15, 2007, aboard Naval Station Norfolk in the SPAWAR Systems Center Charleston Tidewater Node of the FORCEnet Composeable Environment.

Trident Warrior happens to have numerous threads that will attempt to answer your question. We have several interagency objectives within the Truman Strike Group and facilities ashore, and we are even working with nongovernment organizations, such as the World Health Organization, to better develop technologies and processes to ensure they are included as well.

People that lack the ability to discuss issues with the media have missed the interagency bit. I have done it on a number of occasions in my career, and we have to make sure that we get that message quite clear and correct.

A lot of military people almost feel afraid of the media and media coverage. I don't know why because this is your opportunity to get them on your side and to declare and demonstrate and get their support so it gets publicized. You send the message and more people see the message and read the message. That's my personal point.

CHIPS: How are the experiments going? Are there any surprises or early successes or disappointments?

CDRE Cleary: Trident Warrior has been a tremendous success, though there have been a few disappointments here and there. Although analysis is ongoing, the 'quick-look' reports have given us a very good sense that we identified many important lessons, in both technologies and processes, that we will be able to implement in short order.

The multinational MOC to MOC coordination and cooperation resulted in an immediate improvement in our ability to work together across the regions, something I hope we are able to institutionalize in doctrine and tactics, techniques and procedures, as soon as possible. Many technologies highlighted significant gains in terms of information sharing and situational awareness.

We are now in the difficult business of analyzing what worked best, in what conditions. Some we will no doubt want to adopt. Some we will want to reject. Some we will identify for continued testing. What we confirmed, without a doubt, is that we can't fight tomorrow's problem with yesterday's tools, methods and ideas.

Go to http://www.secondfleet.navy.mil/files/leadership/dep_dir_csf.html, for a copy of Commodore Cleary's biography. CHIPS

Q&A with Commander, Navy Region Southwest Rear Adm. Len R. Hering Sr.

Rear Adm. Len R. Hering Sr.

The core business areas for Navy Region Southwest include human resources management, legal, administrative processes, public affairs, religious programs and business and financial management sub-functions, ship movements, harbor craft repair and logistics. CNRSW's mission area includes operations in Southern California at the San Diego Metro: Broadway Complex, Naval Base Coronado, NAVBASE Point Loma and NAVBASE San Diego. Other California locations include: Naval Air Facility El Centro, NAVBASE Ventura County, Naval Weapons Station China Lake, NWS Seal Beach, NWS Seal Beach-Detachment Corona, NWS Seal Beach-Det Fallbrook, NWS Seal Beach-Det Concord, Naval Air Station Lemoore and the Naval Postgraduate School.

CHIPS: Can you talk about the scope of your responsibilities?

Rear Adm. Hering: The Navy Region Southwest is an echelon III command responsible to Commander, Navy Installations Command (CNIC) for the execution of Base Operating Support (BOS) for the fleet, family and fighter. We are responsible for maintaining and supporting all the infrastructure of the Southwest region, which has grown in size. We are now six states in the Southwest United States — Arizona, New Mexico, Nevada, Colorado, Utah and California — six big states.

CHIPS: What technology tools does CNRSW use?

Rear Adm. Hering: We are always looking for new technology. We have quite a few technologies that have been deployed and are helping us to manage our resources. They include things like our Total Workforce Management System, referred to as TWMS, which helps us to manage and access records for our personnel.

At the echelon II level, CNIC is developing a transitional hosting center which allows us the opportunity to manage our database and servers better on the Navy Marine Corps Intranet architecture. We are excited because that allows us to get to the next step and that is the transition from legacy applications to a supported operation that is consistent.

We are looking for a number of different opportunities in technology that can minimize and enhance the need for personnel in executing our antiterrorism force protection requirements — cameras, things like SmartGate and Blue Force locators — that allow us to manage our force in emergency management situations. We are also interested in biometrics for identification and support of those antiterrorism force protection requirements.

We are looking for things that help us manage our BOS better, technologies that will allow us the opportunities to incorporate our pass and ID system better and opportunities for us to manage our telephone systems better and more effectively. We just finished a business case analysis for voice-over-IP. We see a huge potential in being able to manage our base communications in the existing infrastructure of NMCI or the next generation — that will greatly enhance our capability to communicate with one another.

We are working hard with technologies that help us do our business better. We manage a database system called RSIP, the Regional Shore Infrastructure Planning support system, which is the backbone of our GIS, or Geographic Information System, capability on which every piece of our planning requirements resides. Additionally, they help us with our future plans. Navy Ashore Vision 2030, developed by the CNO (Chief of Naval Operations) two years ago, utilizes that GIS technology to help us manage the infrastructure of the 21st century Navy.

We are relying on technology. We need to be aggressive in how those technologies can help us in the future and be willing to look at solutions that include technology as we move into the 21st century. It is the force-multiplier.

CHIPS: What organizations do you work with?

Rear Adm. Hering: We have a large requirement to operate in the emergency management realm. Our responsibility lies with each of the six states that I mentioned. My job is to be a coordinator for the defense civil support authorities that may be required of us in the terre ferme. It is our responsibility. I have emergency preparedness liaison officers, referred to as EPLOs, who are responsible to each of the particular states that they are operating in who should be cognizant of their plans and execution responsibilities and how I might plug into those plans if a disaster were to occur.

I also deal with some of our folks down south, our border partners in Mexico. We have a tie there between their law enforcement and our border shore patrol, and we also support the National Guard working at the border.

We host many of our coalition partners as they come through the area. That is an exciting part of our job. We are able to interact with those folks and show them how we do business, and we learn through that partnership how they operate and how we can help them out as we look to the future.

Areas of concern include the global war on terror, which is in the forefront of everything we do. We are focused on making absolutely certain that we have a proper balance and that our attentions are always toward the fleet, fighter and family. Those concerns are mixed with the concerns of being able to manage a limited budget and resource allocation that cause us to be careful with the way we execute our requirements. Our biggest concern is making sure that we have the mix right and that we have applied the right resource at the right level to provide the right readiness.

CHIPS: Does the CNRSW provide humanitarian assistance?

Rear Adm. Hering: We would provide humanitarian assistance if we were called to do so. We do have a tremendous outreach in the local community. We sponsor a huge number of volunteers in our school programs and in our local baseball and basketball leagues. We are involved heavily in environmental projects in and around the bay and throughout the region. We have a lot of opportunities with our neighbors in making sure that we are an active part of the community. We have the capability of providing humanitarian assistance and support should they need it, but we really look for the day to day interaction with the community. We are inextricably linked to the local community. CHIPS

Designing a Network to Empower the Fleet

Challenges, Opportunities for NNFE Year 2

By Steven A. Davis, SPAWAR Public Affairs

The FORCEnet construct began as a systematic methodology for the Navy to optimize information for tactical advantage. Since the early days of the Copernicus concept for redesigning post Cold War C4I, or command, control, communications, computers and intelligence, the role of the network and technology was a means to an end rather than the ultimate goal.

The "center of the universe" was, and remains, the warfighter. But the challenge continues to be the development of the most capable, effective network to empower the warfighter with a superior edge over an adversary.

Early in his tenure as Chief of Naval Operations, Adm. Michael Mullen challenged Navy leadership to improve readiness, to become more efficient, and to identify resources to recapitalize the future Navy. In response, each of the Navy's acquisition organizations that support the air, surface, submarine, expeditionary and network communities realigned under an enterprise model to improve speed to capability for the fleet at the right cost.

"We can't stay bogged down in discussing network-centric versus platform-centric warfare," said Mullen in January 2006 at a major defense conference held in San Diego. "We must design the fleet to exploit the network and design the network to empower the fleet."

The NNFE Is Born

To meet the CNO's vision, the Naval NETWAR FORCEnet Enterprise, the Navy's enterprise approach to implementing FORCEnet and delivering network-centric capabilities for the fleet, was established to assess current network-centric capabilities, consolidate, or eliminate systems where advantageous, and to recapitalize funds for initiatives that will directly address the needs of Sailors and Marines.

An undertaking of this magnitude required collaboration from across the Navy. The Naval Network Warfare Command (NETWARCOM), Office of the Chief of Naval Operations (OPNAV N6), the Space and Naval Warfare Systems Command (SPAWAR) and a host of additional stakeholder organizations were called upon to make it happen.

Much of the NNFE's 2006 efforts have been focused on developing processes and metrics across the enterprise, such as capability-based assessments and gap studies, to help the Navy better understand the costs of conducting business and how these costs relate to readiness.

This approach will allow the enterprise to make better decisions when applying critical resources — both dollars and manpower — and provide the right products and services to the fleet faster and more efficiently.

"This has been an exciting first year for the Naval NETWAR FORCEnet Enterprise, and we are already beginning to see the benefits of this collaborative effort," reflected NETWARCOM Commander Vice Adm. James D. McArthur, who also serves as the NNFE chief executive officer. "While we are still shaping alignment, we are always looking at resources, funding technology in the future, and how we can meet fleet requirements. We are on the cusp of dramatic changes in C4I and making huge leaps in providing capabilities that support the warfighter."

In recognition of the strategic importance of a comprehensive enterprise approach, the Navy Enterprise Executive Committee met for the first time in November 2006 to discuss how to achieve an integrated, aligned and focused enterprise operating model across the Navy.

Composed of senior leadership from the Navy secretariat, the Navy staff and the fleet, the executive committee is laying the foundation for a business model based on measurable outputs, processes, impactful metrics and accountability.

The NNFE's sister organizations — the Surface Warfare Enterprise (SWE), the Undersea Enterprise (USE), the Naval Aviation Enterprise (NAE) and the Navy Expeditionary Combat Command (NECC) — have progressed through varying degrees of maturity. The more established enterprises, such as the NAE and the SWE, have been fully implemented throughout their respective communities for several years. The more recently established enterprises — the USE, NECC and the NNFE — are beginning to assess their communities' landscape.

One of the most difficult challenges for the enterprises has been to establish meaningful metrics to assess performance and change behavior. While other enterprises can lay claim to "Aircraft Ready for Tasking" or "Ships Ready for Tasking," the challenges are perhaps greater for the NNFE because C4I capability spans virtually all platforms in the Navy.

The problem is further complicated by the fact that the NNFE is not the sole provider of C4I capability within the Navy — a situation the NNFE would like to change.

A preliminary set of metrics governing the measurement of effective C4I capability has been developed, but it is recognized by NNFE leadership that further refinement and definition of metrics are necessary before they can be published and evaluated by Navy leadership.

A NNFE leadership off-site meeting took place in early March to review progress so far and to evaluate what remains to be accomplished in this vital area. It is one of the highest priorities of the NNFE for its second year of operation.

Chief of Naval Operations Adm. Mike Mullen testifies on the 2008 National Defense Budget Request before the House Armed Services Committee. Mullen joined Secretary of the Navy the Honorable Dr. Donald C. Winter and Commandant of the Marine Corps Gen. James T. Conway in testimony before the committee. U.S. Navy photo by Chief Mass Communication Specialist Shawn P. Eklund.

Adjusting the FORCEnet Model

The enterprise model is changing the culture of how FORCEnet products and services are delivered to the fleet. Success will be determined not through the eyes of the acquisition community but by stakeholders and customers.

SPAWAR Commander Rear Adm. Michael C. Bachmann notes that the definition of customers, the end users of products and services the NNFE delivers, has expanded considerably over the past few years. Combat operations, homeland security and business applications must now be designed with an eye toward inter-service and government agency interoperability, as well as the fleet.

The NNFE must ensure that the products and services delivered fulfill a variety of customers' missions requirements. The key to which is built upon effective and aligned partnerships to maximize capability within cost and schedule.

Bachmann's role as the NNFE's chief operating officer "has afforded me the opportunity to work directly with the fleet in areas that in the past would have been considered outside of my lane," he said.

Bachmann has established a corps of readiness officers who provide critical C4I updates to support deploying carrier and expeditionary strike groups. The readiness officers work with combat systems officers over the Fleet Response Plan cycle to ensure that systems are manned, the ship's crew is successfully trained and the material condition of the systems is as close to 100 percent as possible.

"That's been a real success story — our interactions with the fleet have been very positive," Bachmann said.

Deputy Chief of Naval Operations for Communications Networks Vice Adm. Mark Edwards discusses OPNAV N6's plan to recapitalize funds by replacing Navy legacy systems to reap the huge benefits of new technology and cost savings, and reinvest in the needs of Sailors and Marines. Increased bandwidth capacity for Sailors at sea is just one of Edwards' top priorities. The admiral laid out his plan to an audience at West 2007, co-sponsored by AFCEA International and the U.S. Naval Institute, Feb. 2 at the San Diego Convention Center.

Results from the annual Trident Warrior series of operational experiments have also produced positive results, particularly in the field of Maritime Domain Awareness. Trident Warrior has assessed many technologies since its first experiment in 2003, a number of which have been "fast-tracked" to the fleet. Examples include Subnet Relay and High Frequency Internet Protocol, which are line-of-sight communication systems that support ad-hoc, common operational picture networking between U.S. and coalition forces.

Initiatives such as the Automatic Identification System, a maritime tracking and identification system for vessels based on similar principles employed by air traffic controllers, have proven their value both in terms of capability and rapid deployment.

The Combined Enterprise Regional Information Exchange System-Maritime, or CENTRIXS-M, which allows high-speed data exchange among coalition navies, was also developed and fielded through Trident Warrior experimentation.

These capabilities significantly improve the ability of U.S. and coalition forces to work efficiently and effectively together and are another step on the road to establishing the "1,000-ship Navy" as envisioned by the CNO.

Capturing the Money

In May 2006, the CNO announced a realignment of the OPNAV structure in recognition of the critical role of networks. A three-star deputy CNO for Communication Networks organization was established to serve as the principal adviser for network-centric, C4I, surveillance, reconnaissance, space, information operations, information assurance and business information systems.

"Networking the naval warrior through communications networks has become a linchpin in effective leadership for the 21st century," stated Vice Adm. Mark J. Edwards, OPNAV N6 and NNFE chief financial officer. "Getting the greatest return on the Navy's C4 investments requires a unified information technology strategy."

As reported in the CHIPS January-March 2007 issue, one of N6's first initiatives was to identify, migrate and reduce legacy systems in use throughout the Navy. This process is referred to as "capturing the money," or maximizing the Navy's investments in information technology.

Many of the legacy networks in use today use vendor-specific applications or hardware. Through the development of service oriented architecture, the Navy can identify a common set of core services that all applications can use. Thus, shore sites, and particularly ships at sea,

Dr. Dov S. Zakheim, former Under Secretary of Defense (Controller) and chief financial officer for the Department of Defense speaks with Vice Adm. John G. Morgan, Deputy Chief of Naval Operations for Information, Plans and Strategy, and Rear Adm. Michael C. Bachmann, commander of the Space and Naval Warfare Systems Command, during a luncheon panel at West 2007. U.S. Navy photo by Mass Communication Specialist Seaman Omar Alexander Dominquez.

which have a finite amount of data storage capability, can reduce the number of networks required to operate applications while concurrently increasing the number of applications that run on the reduced number of networks.

The NNFE has embarked upon an ambitious course to deliver widespread service oriented architectures to the fleet. As Bachmann explained, "We want to get to the position where we tell the Marines, 'Don't bring your systems on board, just bring your software. We'll load it for you, we'll host it, we'll protect it — and you will have uninterrupted service.' "

By reducing the number of networks needed to operate systems and applications, the Navy can then recapitalize resources into critical needs that the warfighter has already identified, such as improved bandwidth and satellite communication availability and real-time collaboration capabilities.

Reinvesting funds into Navy initiatives, such as Sea Warrior, which allows Sailors at sea to complete long-distance education, training and orders processing requirements, is high on the list of NNFE priorities.

"It is my intent to find IT investments that not only meet our warfighting requirements, but also provide our Sailors with the access they need to advance their careers and conduct their personal lives," Edwards said.

Today's bandwidth availability on Navy ships presents both mission and quality of life challenges. Edwards has noted that computers aboard aircraft carriers download information at 3.7 megabytes per second, while cruisers download at 0.64 megabytes per second and destroyers download at 0.128 megabytes per second. In comparison, the average college campus can download information at more than 45 megabytes per second and the average cell phone downloads at .4 megabytes per second.

Therefore, maximizing bandwidth is key to ensuring that a technologically savvy generation of Sailors and Marines is not disadvantaged while at sea. "It's hard for our new Sailors not to be discouraged when they find out that our cruisers, destroyers and frigates have less bandwidth than they typically have at home or on their cell phone," Edwards explained.

Shipboard and strike group networks have evolved to an essential part of the sensor-to-shooter information chain. Not surprisingly, networks have further evolved into providing far-reaching quality of life, educational, and recruiting and retention support. They are essential in coalition operations and in working with other federal agencies in support of homeland defense.

NNFE leadership and the organizations they represent have made tremendous progress. They have established discipline in the procurement process where there was little; they have brought rigor to discussions of capability, entitlements and requirements where there were none; and they have planned a roadmap for the future. The task will continue to be challenging because information technology is the fastest growing, most rapidly changing element of our society.

The needs are many, but the NNFE is dedicated to providing all these tools, and more, to the warfighter. CHIPS

NSIPS Now Available Fleetwide

By the PEO-EIS Public Affairs Office

The Program Executive Office for Enterprise Information Systems released a quality-of-life enhancement that became available fleetwide on February 7 with the final shipboard installation of the Navy Standard Integrated Personnel System (NSIPS).

As the Navy's Web-enabled pay and personnel management system, NSIPS provides field level standardized and integrated pay and personnel records management capability for all 374,687 Navy active and Reserve members. The final installation occurred aboard the USS Kitty Hawk (CV 63) and marked the achievement of full operational capability — the last major acquisition milestone for the NSIPS program.

"The ability to easily and reliably access their pay and personnel records from around the fleet is an immense enhancement because it gives our Navy members a tool to help manage their career," said Cmdr. Susan Eaton, NSIPS program manager. "Having NSIPS and the Electronic Service Record (ESR) available fleetwide enables timely and accurate pay changes and provides Sailors at sea or shore commands with ready access to their service record data. Sailors can focus on their mission rather than worrying about whether or not their records are up to date."

In October 2006, the Chief of Navy Personnel (CNO N1) authorized the use of the ESR for service record management. ESR replaces the current paper-based Field Service Record with an electronic records management application. It automates most service record maintenance, and provides individual service members with secure Web access to service record data.

ESR was initially deployed to the Navy Reserve in February 2004, providing Reservists with the capability to update civilian employment information.

The system ensures unprecedented safety and security of Navy pay and personnel records by requiring individual validation for entering, changing, viewing and downloading information.

NSIPS utilizes state-of-the-art technology with a defense-in-depth and multitiered architecture to provide maximum data safety and security from external threats. NSIPS is the only Navy program that is completely hosted on the Navy Marine Corps Intranet (NMCI) for the shore component of the application. The system is operational at 351 shore sites and on 151 ships.

The PEO-EIS develops, acquires and deploys naval enterprise-wide networks and information systems. This portfolio of projects and programs include the NMCI, Navy Enterprise Resource Planning (Navy ERP), Global Combat Support System-Marine Corps (GCSS-MC), Total Force Authorizations and Requirements System (TFARS), Navy manpower and personnel programs and NSIPS.

These programs provide information technology capabilities as well as enable common business processes to Sailors, Marines and the organizations that support them.

For more information go to the SPAWAR Web site at http://enterprise.spawar.navy.mil and click on the PEO-EIS program seal. CHIPS

CAN YOU HEAR ME NOW?

HOST NATION COORDINATION:

ASSURING SPECTRUM SUPPORTABILITY OUTSIDE THE UNITED STATES

By the DON CIO Telecom/RF Spectrum/Wireless Team

Obtaining foreign spectrum support for Marine Corps and Navy operations is referred to as "Host Nation Allocation" (HNA) or "Host Nation Coordination." Regardless of the term used, acquiring host nation spectrum supportability from foreign nations is critical to the training and operations of the Department of the Navy (DON), and it is a complex and lengthy process.

Earlier this year, the Joint Staff Director for Command, Control, Communications and Computer Systems (J-6) stated that 51 percent of new Department of Defense (DoD) systems procured in fiscal year 2006 use electromagnetic spectrum. Most DON weapons systems, communications systems, sensor systems, and intelligence systems use electromagnetic spectrum, including radio frequencies, infrared frequencies and more, in some manner.

Obtaining frequency assignments to operate within the United States and its possessions (US&P) is generally not a challenge because the majority of spectrum-dependent systems procured from U.S. sources conform to U.S. frequency allocation. However, obtaining spectrum supportability for operations outside the US&P is too often problematic.

There are two fundamental factors which must be understood when acquiring host nation spectrum support:

Sovereign Nation Spectrum Rights: The fundamental law of international spectrum is that each and every sovereign nation has the undisputed right to manage and use the electromagnetic spectrum within its borders as it deems appropriate.

Spectrum Allocations: The International Telecommunication Union (ITU) is the international organization within the United Nations that develops international regulations "to ensure rational, equitable, efficient and economical use of the radio-frequency spectrum." The ITU establishes global allocations of electromagnetic spectrum, or radio frequencies, that are intended to support specific types of services: mobile and fixed communications, maritime communications, radar and more, and minimizes harmful radio frequency interference.

ITU spectrum allocations are implemented in most countries throughout the world. Frequency allocations that support specific systems or capabilities within the United States often conflict with frequency allocations in other countries. If these conflicts are not resolved, the result could be radio frequency interference that degrades the capabilities of both host nation and DON systems.

To prevent interference, host nations regularly place restrictions on DON electromagnetic spectrum use within their country. Host nation restrictions, such as terminating radar operations when Navy ships enter host nation waters or limiting frequency-hopping capabilities, can degrade the capabilities of DON equipment.

Although the U.S. equipment certification process is usually not referred to as host nation spectrum supportability, the United States is, in fact, the host nation. Generally, the military services request certification of all spectrum-dependent systems when they are being acquired. The process requires the submission of equipment parameters, including transmitter power, bandwidth, and more, to the National Telecommunications and Information Administration (NTIA), which validates that the equipment operates within U.S. spectrum allocations and is supportable within the US&P. The equipment is then certified and frequency assignments can be obtained for operation within the US&P.

Obtaining host nation spectrum support outside the US&P is similar to the US&P process except that the geographic combatant command (COCOM) is responsible for coordinating host nation spectrum supportability. Again, the military services initiate the process by providing the technical parameters to one or more COCOMs, instead of the NTIA.

The COCOMs operate with the consent of the U.S. State Department and provide the parameters to the host nations. If U.S. equipment conforms to a host nation's spectrum allocations, it generally supports the request. However, sovereign rights and multiple services within a given ITU allocation often prevent naval equipment from receiving host nation coordination, despite the equipment being certified within the United States.

There is no guaranteed process to ensure all DON systems certified for use in the United States will receive carte blanche spectrum supportability abroad. However, by following these recommendations, the DON can greatly improve the likelihood that spectrum-dependent systems will be supported in host nations.

Organizations procuring spectrum-dependent systems should:

– Consider spectrum supportability up-front in the acquisition process and consider it as a Key Performance Parameter (KPP).

– Determine where the equipment will be used and conduct the appropriate research to understand the spectrum allocations of those countries.

– Solicit the expertise and assistance of the Joint Spectrum Center, go to http://www.jsc.mil, for more information.

Spectrum access throughout the world is critical to the naval services. Understanding the challenges and processes associated with host nation spectrum support enables organizations involved with the acquisition of spectrum-dependent devices and systems to implement necessary controls that ensure the Marine Corps and Navy remain the most capable military forces in the world. CHIPS

Ike Sailors Take Part in Astronomical Reenlistment

By Mass Communication Specialist 2nd Class Matthew D. Leistikow

USS Dwight D. Eisenhower (CVN 69) at-sea Sailors and embarked Carrier Air Wing (CVW) 7, participated in a historic reenlistment ceremony of astronomical proportions when astronaut and U.S. Navy Capt. Michael Lopez-Alegria, commander of the International Space Station (ISS), presided over the ceremony from space Jan. 29 via video teleconference, along with astronaut and U.S. Navy Cmdr. Suni Williams, ISS flight engineer.

Sixteen Sailors became the first from the Ike to be reenlisted by an officer from NASA in a ceremony which crossed Earth's atmosphere to the ISS orbiting at 200 miles above. The VTC included the ISS, Ike, NASA and a Norfolk, Va., site for families to participate.

"It's pretty exciting," said Aviation Boatswain's Mate (Aircraft Handling) 3rd Class Dubiell De Zarraga, from Ike's Air Department, V-1 Division. "I'm pretty sure I'm going to remember this for the rest of my life — and my family will also."

Ike's commanding officer, Capt. Dan Cloyd, and Lopez-Alegria crossed paths through mutual friends just before Lopez-Alegria's mid-September launch for the ISS. They both became determined to find special ways to bring the ISS and Ike crew together.

"The space station and Ike have a special bond in that before he left, Michael took along two commissioning pennants from the ship," Cloyd said. "He is holding one for him and the space station, and one he will present upon his return to us."

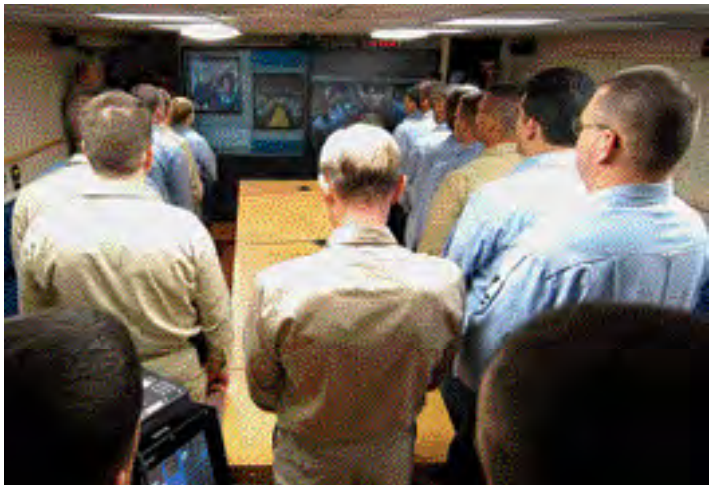
Cloyd and Lopez-Alegria worked together to help create a unique experience for an important event in a Sailor's career.

"Everybody always wants to make their reenlistment special," Cloyd said. "This was a great idea as well as an opportunity to do something historic."

Lopez-Alegria felt it was a special honor to take part in a crucial point in a Sailor's naval career.

"We really feel close ties to the Navy and unfortunately it's difficult to maintain those ties given our jobs — and certainly given our locations. This is a great opportunity for us to share this with you," Lopez-Alegria said.

Orbiting 200 miles above Earth, astronauts, Navy Capt. Michael Lopez-Alegria, commander for the International Space Station, and flight engineer Navy Cmdr. Suni Williams reenlist 16 Sailors aboard the Nimitz-class aircraft carrier USS Dwight D. Eisenhower (CVN 69) via video teleconference.



Aviation Electronics Technician 3rd Class Courtney Busdeker and 15 other Sailors aboard the aircraft carrier USS Dwight D. Eisenhower (CVN 69) repeat the Oath of Enlistment during a historic reenlistment ceremony Jan. 29, 2007, led by Navy Capt. Michael Lopez-Alegria, commander of the International Space Station.

Before Sailors could raise their hand and solemnly swear to defend America's Constitution, people from numerous commands had to work together to make the event possible.

Cmdr. Zig Leszczynski, space operations officer for the Eisenhower Carrier Strike Group, helped put Ike coordinators in contact with the right people at NASA by working through a friend at NASA, astronaut and Navy Capt. Chris Ferguson.

The Ike CSG is the 2nd Fleet executive agent for space, in support of the Naval Space Campaign, which aims to incorporate space capabilities in naval operations.

"It's easy for me to go through the Navy Space Cadre, a network of space professionals throughout the Navy, including NASA astronauts, to make sure this happened," Leszczynski said. "This is one of many times we were able to use the Space Cadre network to accomplish the mission."

Leszczynski said the reenlistment was symbolic of the history the Navy has had in space.

"The Navy has a great heritage in space," he said. "This ceremony is one way that this great Navy heritage continues."

The event also allowed some of the Sailors a chance to see their loved ones in Norfolk, Va. Family members woke up before sunrise to participate.

Each Sailor reenlisted for his or her own reasons, but using naval space technology to connect Sailors to outer space and back home helped make reenlisting a special experience.

"I've passed on some opportunities before because I had work to do," said Chief Aviation Structural Mechanic (AW) Richard Klein from the "Wildcats" of Strike Fighter Squadron (VFA) 131. "But this was something I wasn't going to pass up on. It's cool for me to be a part of something that's never been done before."

The Sailors reenlisted for a total of 57 years, and some of them received a reenlistment bonus from a combined total of more than $42,700.

CHIPS

How we reached into space

By Cmdr. Brian Julian

USS Dwight D. Eisenhower (CVN 69) at-sea Sailors and embarked Carrier Air Wing (CVW) 7 participation in the memorable reenlistment ceremony required hard work and planning. Linking the ship-air wing at sea in the Indian Ocean, the International Space Station in orbit several hundred miles above Earth, and families and news media on the ground in Norfolk, Va., took precise coordination and technological know-how to ensure the success of the historic reenlistment ceremony from space.

With only a 19-minute video connection window of opportunity with the ISS due to orbital patterns, all the technical coordination had to be solidified days before the event.

A video teleconference from a ship at sea requires bridging at a shore-based communications facility because the unique transmission equipment installed on a ship is not directly connectable to the commercial VTC suites widely used by other organizations. To effect connection to the ISS, several shore-based "hops" were necessary.

The transmission method used by the Ike was over a Super High Frequency (SHF) satellite link to the Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT) in Norfolk, Va.

Once the ship and the communications station are connected by satellite (referred to as the path), a number of different circuits used in a variety of applications can be passed over the path and transmitted further all over the world using a system called Timeplex. Timeplex is a multiplexing system that takes different types of data feeds, for example, voice, data, serial, T1 lines and Ethernet, and merges them into a single data feed for wide transport.

The ship's VTC signal was placed on the SHF transmission path to NCTAMS LANT, which was then passed over a Timeplex internodal link to NCTAMS LANT Detachment Hampton Roads to enable the signal to be further transferred to the bridge.

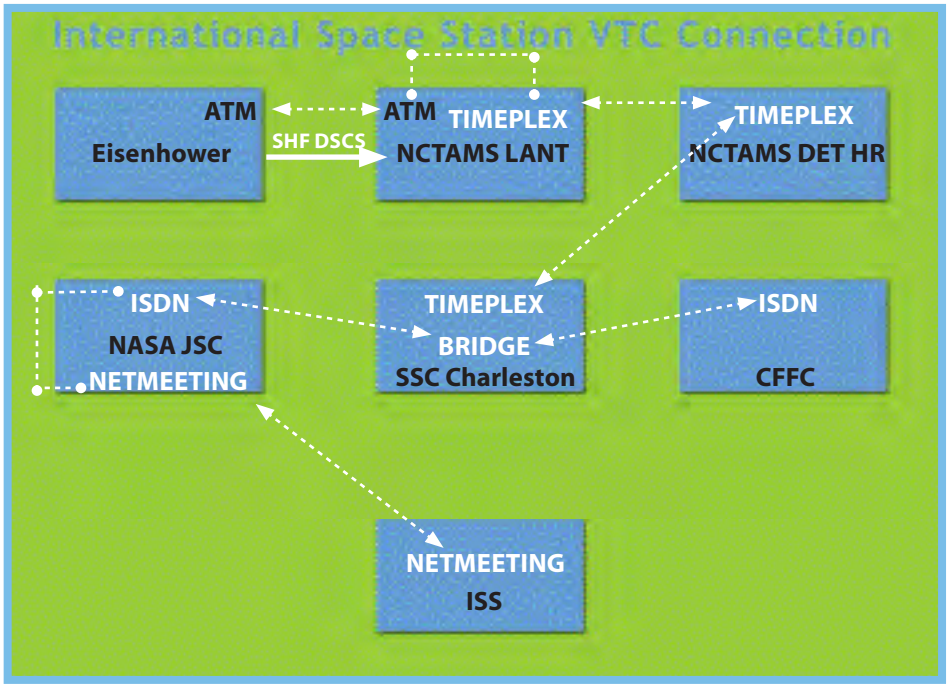


Figure 1. International Space Station VTC Connection.

The Space and Naval Warfare Systems Center (SSC), Charleston, S.C., served as the VTC bridge that connected all participants together.

The NASA Johnson Space Center established a link with SSC Charleston's bridge through an Integrated Services Digital Network (ISDN) phone line. Norfolk's Fleet Forces Command also used an ISDN connection to the SSC Charleston bridge to enable the families of the reenlisting Sailors and Norfolk area media to watch the reenlistment, and later talk to Sailors.

Once all the technical connections were made and participants verified good audio and video with each other, NASA completed the circuit by patching through a Windows NetMeeting video with the astronauts into the VTC. Figure 1 illustrates the configuration.

The reenlistment was a huge success, and there was even time left for the astronauts to answer questions from the reenlistees and news media.

Cmdr. Julian is the combat systems officer for the USS Dwight D. Eisenhower. For more information go to the Ike's Web site at http://www.eisenhower.navy.mil. CHIPS

This unique ceremony was made possible by an extraordinary team of professionals from the USS Dwight D. Eisenhower and each of the organizations listed below.

USS Dwight D. Eisenhower (CVN 69)
ITC (SW) Steven Booker - Technical Control
Lt. Cmdr Carla McCarthy - Public Affairs Officer

Commander Carrier Strike Group Eight
Cmdr. Zig Leszczynski - Space Cadre

NASA Johnson Space Center
Ms. Gabrielle Avina
Mr. Duane Chin
Mr. Christopher Van Velson
Ms. Erin Taschner
Ms. Ginger Kerrick
Ms. Shannon Walker

Commander Fleet Forces Command
Ms. Robin Bedford

SSC Charleston
Mr. Rod Knapp

NCTAMS LANT Detachment Hampton Roads
CWO3 John Fedele
IT1 Juan Ramos

NCTAMS LANT
CWO3 Curtis Smith
IT1 Kenneth Cox

Introducing the Next-Generation Common Access Card

By Sonya R. Smith

The Department of Defense (DoD) is modifying the current Common Access Card (CAC) to meet the mandates of Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 establishes a federal standard for identification credentials issued to all federal employees and eligible contractors.

The "next-generation CAC" is being phased in throughout the DoD as current CACs expire. During this transition period, both the current Common Access Card, and the next-generation CAC will be in circulation. Both are valid forms of identification and there is no benefit to replacing your current card with a next-generation CAC before its expiration date.

The next-generation CAC maintains all the capabilities and functionality of the current card: data stored on an integrated circuit chip (ICC) enables rapid electronic authentication and enhanced security. PKI certificates generated and stored on the card enable the card owner to digitally sign documents and e-mails, encrypt e-mails, and establish secure online network connections.

Added Functionality

Instead of having to stop and "swipe" your card to read the information from the magnetic stripe or bar code, the next-generation CAC adds a contactless technology capability, which provides the ability to utilize radio frequencies to transfer data between the card and the card reader for physical access. This increases the speed for identity authentication and improves the ability to manage heavy traffic flow into facilities.

In addition to the PKI certificates, the next-generation CAC adds biometrics in the form of a digital photo and two index fingerprints, stored as minutiae templates on the ICC. The minutiae templates are a mathematical representation of the data points unique to each set of biometrics. They are used instead of storing actual fingerprint images on the next-generation CAC to protect against compromise.

Biometrics provide the ability to positively bind the individual to his or her credential. The integration of biometrics and PKI with the CAC provides an added multifactor authentication capability for logical and physical access systems.

Multifactor authentication, which relies on more than one means to authenticate identity, is a more robust authentication scheme because it requires possession of a particular item — the CAC; knowledge of a particular item — your Personal Identification Number (PIN); and physical verification — biometrics.

Changes in Appearance

The look of the next-generation CAC will change slightly to meet federal standards and to better meet security needs. Figure 1 shows a depiction of the current CAC on the left and the next-generation CAC on the right. The following are the key differences you will see with the next-generation CAC:

Color Coding:

- *A red stripe will be used to represent first responders. Red is used to identify foreign nationals on current CACs.*
- *A blue stripe will be used to represent foreign nationals.*
- *A green stripe will continue to represent contractors.*
- *The stripe will be horizontal under the photo and fade from light to dark. Currently the stripe is vertical on the right side.*

Data Storage

Contrary to popular belief, the CAC does not store any personal or medical records. The next-generation CAC requires increased storage capacity simply to store the biometrics and the federally required Personal Identity Verification (PIV) certificate. The goal, in our net-centric world, is to use the card, with its PKI and biometrics as identity authentication factors, to access authoritative data sources through Web portal applications. Below is a summary of the key data included in the technology of the card.

The integrated circuit chip stores 64 kilobytes of data, including:

- PKI certificates
- Two digital fingerprints (minutiae templates)
- Digital photo
- Personal Identity Verification (PIV) certificate
- Organizational affiliation
- Agency
- Department
- Expiration date

Bar codes may store key personal information, including:

- Name
- Social Security Number
- Date of birth
- Personnel category
- Pay category
- Benefits information
- Organization affiliation
- Pay grade

The magnetic stripe is reserved for Service/Agency use.

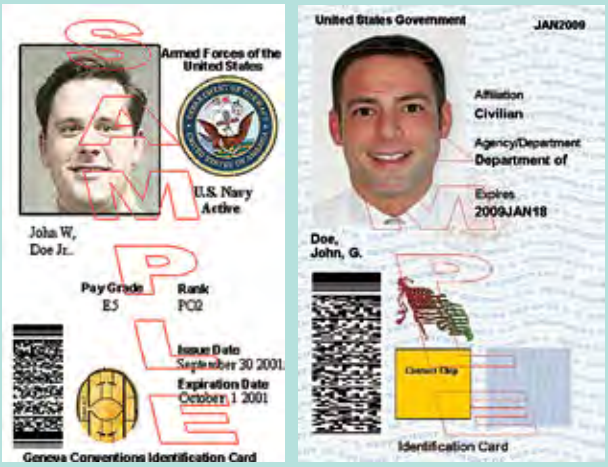


Figure 1 depiction of the current CAC and next-generation CAC.

Getting the Card – Changes to the Process

One of the key mandates of HSPD-12 is that the identity credential must be issued based on sound criteria for verifying an individual's identity. Accordingly, a next-generation CAC can only be issued when a National Agency Check with Inquiries, or equivalent, is submitted and the results of the FBI National Criminal History Check (fingerprint check) have been completed and approved.

When a record has been established in the Defense Enrollment Eligibility Reporting System (DEERS) and the FBI fingerprint check has been completed and approved, individuals must bring two forms of approved identity source documents with them for CAC issuance. *Go to http://www.cac.mil for a list of approved identity documents.*

At least one document must be a valid state or federal government–issued picture identification, such as a passport, driver's license or current/expired CAC. Additionally, just as with the current CAC, you will need a six- to eight-digit PIN and an official work e-mail address in order to receive all your PKI certificates.

Impact to Users

The next-generation CAC requires upgrades to our current middleware infrastructure — the software application that interfaces between host applications, such as e-mail, cryptographic logon, Web browsers, and PK-enabled applications, and the CAC. While DoD upgrades the infrastructure to produce the next-generation CAC, new cardstock is being introduced for the current CAC to replace depleted cardstock inventories.

This new cardstock also requires upgraded middleware for proper functionality. NMCI is upgrading the CAC middleware from ActivClient 5.4 to ActivClient 6.0 during the first quarter of 2007. This upgrade makes NMCI compliant with industry standards and provides support for the next-generation CAC.

If users are issued a CAC with the new cardstock or a next-generation CAC before their NMCI workstation has been upgraded to ActivClient 6.0, they may not be able to use their newly issued CAC on their workstation. Should this occur, the affected users should call the NMCI Help Desk (866-THE-NMCI), indicate they were recently issued either a CAC with the new cardstock or a next-generation CAC, and the NMCI Help Desk will push the ActivClient 6.0 upgrade to the user's workstation. Users not on NMCI who are using ActivIdentity 2.2 should not be affected.

Because the CACs created with the new cardstock look identical to the current version of the CAC, users will only be able to identify the new cardstock by the manufacturer and card type indicated on the back of the CAC. If the CAC reads "Oberthur Card Systems ID-One Cosmo v5.2 72K" above the magnetic bar on the back of the CAC, then the user has the new cardstock.

Users will be able to more easily identify the next-generation CAC because this card will look different from the current version of the CAC, as illustrated in Figure 1.

Different but the Same

The CAC has been well integrated into the DoD with military members, civilians and contractors using it for logical and physical access and digitally signing and encrypting e-mail. It is also used as the standard ID card and Geneva Convention Card.

The next-generation CAC builds upon a proven record of success and meets the federal standards of HSPD-12. Issuance of next-generation CACs began in October 2006 with an Interim Operational Capability solution and will be phased in throughout the DoD as current CACs expire. While there are differences in appearance and functionality, both the current CAC and the next-generation CAC are valid forms of DoD identification.

Ms. Sonya Smith supports the DON CIO information assurance team.

CHIPS

Go to the following Web sites for further guidance:

- HSPD-12, Homeland Security Presidential Directive, August 27, 2004, Subj: Policy for a Common Identification Standard for Federal Employees and Contractors: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.
- FIPS201-1 – Federal Information Processing Standard 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006: http://csrc.nist.gov/.
- DoD Common Access Card Web site: http://www.cac.mil.

Navigation Nugget

New chip-scale atomic clock plus GPS receiver transforms navigation

By Randy Rollo

The Global Positioning System and Navigation Systems Division (Code 231) of the Space and Naval Warfare Systems Center (SSC) San Diego is incorporating a chip-scale atomic clock (CSAC) into a new GPS receiver design that they are calling the "Navigation Nugget."

SSC San Diego's Central Engineering Activity (CEA) Laboratory received the first chip-scale atomic clock from the National Institute for Standards and Technology (NIST) Laboratory last year and will start characterizing a new CSAC from Symmetricom Corp. in April.

Navigation Nugget project manager Randy Rollo said, "The Navigation Nugget is the first GPS receiver in the world to incorporate a CSAC. This is a major milestone that is expected to transform military GPS receiver designs for the future years to come.

"Many battlefield assets, [including the] Global Information Grid-enabled networks and the nation's infrastructure, rely heavily on GPS for timing information and synchronization. GPS is a highly accurate positioning, navigation and timing [PNT] system, but susceptible to interference and disruption."

Navigation Nugget Description

The "Nugget" is the convergence of a chip-scale atomic clock combined with a deeply integrated microelectromechanical systems (MEMS) inertial measurement unit and a GPS M-code software receiver. MEMS is the integration of mechanical elements, sensors, actuators and electronics on a common silicon substrate through microfabrication technology. While the electronics are fabricated using integrated circuit process sequences, the micromechanical components are fabricated using compatible micromachining processes that selectively etch away parts of the silicon wafer or add new structural layers to form mechanical and electromechanical devices.

Technology

The Navigation Nugget creates a robust PNT sensor suite capable of operating in impaired and threatened GPS environments. It will help ground forces in canopy or jammed environments and improve vertical accuracy in differential GPS. Therefore, it benefits antenna systems using beam forming techniques and programs, like the Joint Precision Approach and Landing System, that have stringent vertical requirements. The ability to act as a platform precise timing source is also beneficial to warfighter communications and networks.

The first chip-scale atomic clock evaluated was developed by NIST through the Defense Advanced Research Projects Agency (DARPA) Micro-Electro-Mechanical Systems (MEMS) Program Office. SSC San Diego is the first to incorporate CSAC into the breakthrough GPS receiver design.

The Navigation Nugget core technology fuses a GPS software defined receiver (SDR) with an inertial measurement unit (IMU), all synchronized by the onboard atomic clock to create a robust PNT sensor suite. (See Figure 1 for a diagram of the Navigation Nugget design.)

The initial design objective is the definition, specification and demonstration of an atomic clock's precise time converged with an integrated IMU and the new military GPS (M-code) SDR. The

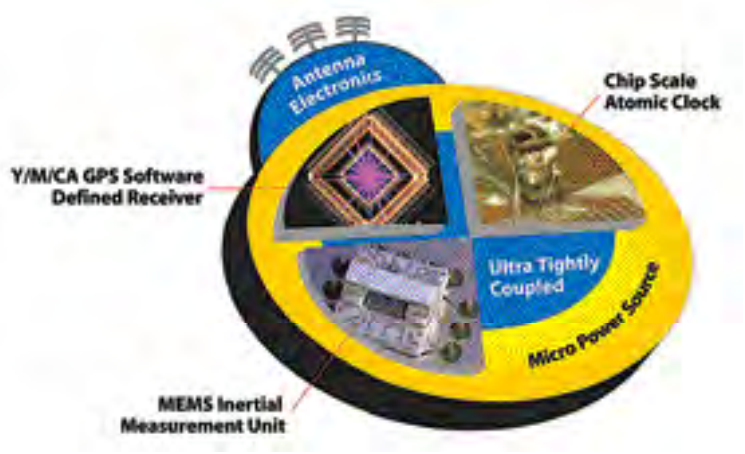


Figure 1. Diagram of the Navigation Nugget.

Navigation Nugget's development cycle is bifurcated into MEMS technology and existing scale components until MEMS technology is fully mature. This allows measurement and validation of the Navigation Nugget's design and benefits and enables larger platforms to receive the improved PNT capability more rapidly. It also allows networks to obtain another source of highly accurate timing. Rollo stated that a field testable prototype could be developed in about 18 to 24 months.

Development and testing is performed in the GPS Central Engineering Activity Lab using a newly developed M-code software defined receiver, inertial navigation system (INS) equipment and atomic clocks. The CEA Lab provides modernized and legacy GPS signal environments for component and system evaluations. It also provides dynamic test scenarios for measuring and validating the Navigation Nugget in a challenging environment in jamming scenarios.

Using the MEMS inertial measurement unit, the Navigation Nugget can continue to operate during periods of GPS signal disruption in urban canyon areas. When the Navigation Nugget begins to receive signals again, it can quickly reacquire satellite linkage because the chip-scale atomic clock will maintain precise time allowing higher probability of fast reacquisition.

Additionally, the Navigation Nugget's flexible receiver design allows integrating signals of opportunity to further enhance indoor navigation. New precise-time-aided algorithms include Code 231's particle filtering accelerator effort for further navigation solution accuracies.

SSC San Diego is using the existing Alpha Data card with a Xilinx field programmable gate array receiver testbed to provide flexibility in developing nugget-based systems. Code 231 engineers are starting with inertial measurement unit simulations to test integration techniques that allow a phased introduction of technology such as particle filtering to further tie the system design together. This spiral engineering process, shown in Figure 2, is designed to accelerate development, reduce government costs and enable rapid analysis.

Goals

The operational payoff goal is to develop a highly resilient positioning navigation and timing system that takes advantage of a chip-scale atomic clock in an integrated configuration. This can be applied to human assets, networks and other platforms as necessary. The goals are:

Figure 2. Diagram of the Navigation Nugget Development Timeline.

• Improve jamming resistance, integrity monitoring, anti-spoofing and fault detection;

•Direct Y-code and M-code acquisitions through "precise-time aiding";

•Accelerate reacquisitions, especially within challenging environments;

• Modify Kalman filter architecture using precise time aiding, i.e., add particle filtering;

•Improve vertical accuracy for coupled beam-forming antenna integrations, Joint Precision Approach and Landing System, etc.;

•Reduce the number of satellites required for an accurate PNT solution;

•Investigate antenna electronics and micropower (fuel cell) integrations.

Battlespace Benefits

The development of the Navigation Nugget allows warfighters and warfighting platforms to navigate in waters and terrains that can be unattainable with current standalone GPS receivers. It allows warfighters to navigate with less interruptions and faster reacquisitions when GPS signal degradations occur. Further, the Navigation Nugget's precise-time feature enables battlefield synchronization for communication systems and networks.

In future platform integrations, the "Nugget's" ubiquitous positioning, navigation and timing sensor suite will enable net-centric synchronization for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems.

The bifurcated approach to spiral engineering of the Navigation Nugget, developed with MEMS technology, satisfies the size, weight and power requirements of unmanned vehicles and dismounted Soldiers.

The future is here today!

Randy Rollo works in the Global Positioning System and Navigation Systems Division of SSC San Diego as the project manager for the Navigation Nugget.

CHIPS

Matt Nicholson (left), senior engineer, and Randy Rollo, project manager, sitting behind the chip-scale atomic clock test fixture in SSC San Diego's Central Engineering Activity Laboratory.

Navy Simulation Meets the Challenge

By the Navy Warfare Development Command

The crew of the Aegis destroyer knows there is an enemy submarine nearby because the strike group has been tracking it for days, but water conditions have deteriorated, and the boat's electric drive simply isn't generating enough noise. The sea state is such that a periscope will be difficult to detect among the sea clutter. An EP-3 is flying over the area alert for intercepts on the sub's electronic signature, but the crew has been in the air for hours, and the aircraft's fuel state is reaching a critical point where the plane will have to turn for home soon.

The tension in the Combat Information Center is palpable. The stakes couldn't be higher: the safety of more than 20 ships, including two aircraft carriers and almost 15,000 men and women, is on the line.

Suddenly, a report of a faint sonobouy return gives the crew the first hint on the sub's location in more than three hours. Despite the heavy swells coming from the southwest, the ship turns to reposition the search. The crew have the know-how and skills to end the hunt and ensure the safety of the battleforce. They have the will and the equipment to make it work …

And none of this is real.

Planners at the U.S. Pacific and U.S. Joint Forces (JFCOM) commands want to ensure that operational staffs are trained in the most realistic operational environment that can be produced — short of actually deploying vast numbers of troops, ships and aircraft to the field. To accomplish this, they called upon the expertise of the modeling and simulation (M&S) community to make the command post exercise Terminal Fury 07 (TF-07) as demanding and faithful to reality as possible.

One of the commands instrumental in developing simulation fidelity is the Navy Warfare Development Command in Newport, R.I. When it was founded in 1998, NWDC had a problem: One of its missions was to conduct complex experiments to evaluate and further develop new concepts and doctrine. The resources needed for these experiments were significant and not always available. In addition, they often involved technologies that did not yet exist.

The clear answer was to use modeling and simulation aggressively, but the fidelity of existing simulation was minimal. The ability to factor in crucial data elements was fractional compared with the requirements, and it was often not possible to determine the outcome of a decision or series of events due to the limited capabilites similation had to offer.

So the NWDC engineering team began a systematic approach for improving modeling and simulation to produce accurate and reliable results. As the degree of experimentation became more and more complex, the M&S capability to faithfully replicate environmental and operational conditions became equally complex. By the time Fleet Battle Experiment Echo (FBE-E) occurred in 1999, simulations representing forces in the experiment could be networked and federated into a single synthetic warfighting environment through the Joint Semi-Automated Forces (JSAF) simulation system supported by the NWDC.

By the time the command supported FBE-Juliet, part of JFCOM's Millennium Challenge 2002, the fleet saw a nearly seamless blend of a simulated environment that could be combined with live, virtual and constructive forces. It was an impressive display of the potential of M&S to replace scarce real-world assets and costly operational time.

Up until 2003, when the NWDC provided modeling and stimulation to fleet assets, truckloads of equipment and busloads of people had to be transported to a site near the action, and a lab had to be created on-site to operate the modeling and simulation. The preparations for FBE Kilo that year included the development of an M&S lab at NWDC headquarters and a sophisticated networking approach to distributing simulation worldwide. For the first time, NWDC could provide systems-level stimulation to ships at sea anywhere in the world from its home base in Rhode Island.

But the simulations used for fleet training did not compare well with what commands were seeing during the FBEs. At the request of the fleet, NWDC was tasked to investigate the possibility of applying its modeling and simulation expertise to fleet training. The results were dramatic. The NWDC team applied its technology and skill set to creating a vastly enhanced fleet synthetic training environment. This capability was applied to the existing Battle Force Tactical Training program and then expanded to support Battle Group Inport Exercises.

In short order, this was further expanded to support Multiple Battle Group Inport Exercises (MBGIE) which could simultaneously simulate onboard systems on ships assigned to several different strike groups. Ships pierside, in such disparate locations as San Diego, Norfolk, Mayport and Bremerton, could interoperate as if they were at sea together. The effort has advanced synthetic training to the point where the NWDC provides executive management of the Navy Continuous Training Environment.

The most recent application of this technology was during PACOM's 10-day TF-07 series, which demonstrated that this architecture supports simulated training events at every echelon of the Navy and joint command structure — from console operator — to combatant command staff and commander.

Terminal Fury 07 surface simulation sub-area.

The exercise linked staffs at PACOM headquarters, Camp Smith, Hawaii; Joint Task Force 519, Makalapa Compound, Pearl Harbor, Hawaii; Kenney Headquarters, Hickam Air Force Base, Hawaii; III Marine Expeditionary Force, Camp Courtney, Okinawa, Japan; U.S. Seventh Fleet aboard USS Blue Ridge (LCC 19); 1st Corps Headquarters, Fort Lewis, Wash.; 4th Psychological Operations Group, Fort Bragg, N.C.; U.S. Strategic Command, Offutt Air Force Base, Neb.; Commander Task Force (CTF) 70 aboard USS Kitty Hawk (CV 63); CTF 72, Misawa, Japan; and CTF 74 , Yokosuka, Japan.

More than 150 people participated in the 24-hour simulations originating from Newport, which provided enhanced training for the Pacific Command and Joint Task Force 519 staffs in all aspects of crisis planning and procedures in PACOM's area of operations.

Through a federation of M&S organizations across the services, the NWDC provided the maritime elements of the simulated environment and controlled both virtual and constructive forces play during the exercise. In addition, the NWDC provided exercise control and network and technical support.

The federation of modeling and simulation capabilities permitted the integration of the individual service and joint simulation systems during the exercise. NWDC and JFCOM participated through the Joint Semi-Automated Forces simulation. Land forces were simulated in the Joint Conflict and Tactical Simulation, and the Air Force participated through the Air Warfare Simulation.

One of the remarkable features of the federated network is the ability to incorporate individual units and trainers into the simulation. During Terminal Fury, an EP3 Mission Avionics System Trainer and an E2C Weapons Systems Trainer "flew" during simulated operations. Their respective performances fully blended into the constructive operational units generated by the JSAF environment. In addition, the 7th Fleet staff participated in the live command post exercise from its command center aboard the USS Blue Ridge pierside in Yokosuka.

The simulation provided the JTF commander, acting as the Joint Forces Maritime Component Commander, a fully reactive simulation down to the individual tactical platform with sensors interacting in a high fidelity environment, and platforms with realistic tactical loads and operational capabilities. Command and control decisions could be fully developed and analyzed as the employment of the JTF progressed. It was a level of realism that, in the past, could only be achieved through the use of live forces.

In addition to tactical displays that faithfully reproduced the geospatial distribution of the participating forces, realism was further enhanced through the use of unit tactical radio circuitry for communications through voice-over-IP technology. This integrated tactical radio line-of-sight equipment with the Internet so that warfighters could use the same communications gear that they would use in actual operations allowing worldwide transport of the communications between geographically dispersed participants.

The lab at NWDC was a beehive of activity throughout the exercise. Cells provided an exercise control group for the strike group and tactical aviation; blue submarine, carrier and air patrol operations; and technical support. In a separate area, an Intel Cell provided intelligence for both the control and operations teams. In a third area, the Red Cell team mimicked opposition forces and provided specialized support, such as the Theater Battle Management Core Systems (TBMCS) and Global Command and Control System – Maritime.

Members of the Terminal Fury 07 Joint Exercise Control Group, left to right, Cmdr. Charles Strassle, 7th Fleet operational support officer and naval force lead; Capt. Chris Gallagher, Joint Forces Warfighting Center liaison officer to the Maritime Cell; and Lt. Cmdr. Brian Bronk, PACOM liaison officer to the Maritime Cell. U.S. Navy photos by John Woodhouse.

TF-07 marked the first time that the NWDC engineering team introduced the use of a completely reworked interface to TBMCS. This system provides a dynamic method for the air component commander to update air tasking. By using a new JSAF/TBMCS interface, the lab provided an automated process to integrate air operations into the simulation.

Training support for an exercise this large and complex took months of preparation. The December command post event was preceded by more than six months of detailed work that included two weeks of systems testing in August, three weeks of testing in October and a week of integrated operations testing and training immediately prior to exercise commencement to ensure that the Navy Continuous Training Environment backbone and the Joint Training and Experimentation Network could support the demands of the exercise.

Future preparations will be significantly reduced because the interfaces between the services' simulation systems are standardized.

The application of modeling and simulation technologies to earlier war games provided the foundation that drove the evolution to better and more capable technologies to support the demands of Navy experimentation. The Navy soon discovered that this same technology could significantly enhance fleet training at every level of the warfare continuum, so it was a natural development to apply this same level of fidelity to naval and joint exercises.

The Navy Warfare Development Command is tasked with ever more complex support requirements for better experimentation and more realistic training in the modeling and simulation environment.

For more information visit the Navy Warfare Development Command at http://www.nwdc.navy.mil. CHIPS

Enabling Warfighter Mission Assurance through Critical Asset Vulnerability Assessment

By Steve Muck

Since its inception in 2000, a primary component of the Department of the Navy Critical Infrastructure Protection (DON CIP) Program has been identifying vulnerabilities associated with DON critical assets that, if exploited, could jeopardize mission execution. The following article describes the current vulnerability assessment strategy being implemented by the DON CIO in his role as the DON Critical Infrastructure Assurance Officer (CIAO).

Enabling warfighter mission assurance has become an increasingly complex goal, with threats to our troops and facilities becoming more asymmetric, insidious — and ever-present.

As Department of Defense (DoD) guidance on critical infrastructure protection (CIP) has evolved to address the current environment, the DON CIP team's efforts in support of DoD have also evolved. In one key DON CIP area, vulnerability assessment, the DON CIP team now supports the Chief of Naval Operations Integrated Vulnerability Assessments (CNO IVAs) by conducting the relatively new "Defense Critical Infrastructure Program (DCIP) Assessment" as part of a CNO IVA.

In this role, the team assists CNO IVA teams in identifying any weaknesses in infrastructures and interdependencies that could potentially affect an installation's ability to complete its mission essential tasks.

Background

Recognizing the role that supporting foundational infrastructure plays in an installation's ability to perform its mission essential tasks, the DCIP community sought to develop a consistent, "best practices" approach to assessing such infrastructure.

As a result of those efforts, in early 2006, the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD (HD&ASA)) issued a comprehensive set of DCIP benchmarks and standards for use with existing IVA protocols.

DCIP benchmark areas include: energy (electric power, natural gas and petroleum); transportation (roads, rail, aviation, seaports and waterways); water systems (potable, industrial and firefighting); chemical storage and use; heating, ventilation and air conditioning (HVAC); communications; and wastewater.

The CNO IVA-DCIP Assessment focuses on DoD-owned, leased and managed assets but also examines commercial providers outside installation fence lines.

The DON CIP team's past experience in evaluating commercial dependency issues during Naval Integrated Vulnerability Assessments (NIVAs) prompted the Naval Criminal Investigative Service (NCIS) to request CIP team assistance for three CNO IVA-DCIP Assessments during the summer and fall of 2006. Those trial sites were: Naval Air Station (NAS) Oceana in Virginia Beach, Va.; NAS Whidbey Island, Wash., and NAS Sigonella, Italy.

The success of those trials led to a request for similar support for six CNO IVA-DCIP Assessments in fiscal year 2007. Sites selected for these efforts are: Naval Station Guantanamo Bay, Cuba; Naval Surface Warfare Center Dahlgren, Va.; Naval Station Great Lakes, Ill.; Construction Battalion Center Gulfport, Miss.; Naval Weapons Station Earl, N.J.; and Naval Base Ventura County, Calif.

Assessments are tailored to the specific mission and local geography of an installation. The DON CIP team performed a DCIP assessment at Naval Station Guantanamo Bay, Cuba, in January 2007.

In this photo from Jan. 10, 2002, watchtower security teams at Camp X-Ray man positions during a mission rehearsal. U.S. Navy photo by Photographer's Mate 1st Class Shane T. McCoy.

In performing these assessments, the objective of the DON CIP team has been to determine whether vulnerabilities exist within supporting infrastructure networks, and if they do exist, whether their compromise would jeopardize mission execution.

Approach

The DON CIP Team's NIVA approach included three primary phases: pre-assessment research; on-site evaluation and collaboration; and post-assessment analysis/reporting.

This approach, which is complementary to current DCIP methodology, has evolved such that it now also incorporates specific guidance from the DCIP Training Program, implemented by the ASD (HD&ASA) in accordance with DoD Directive (DoDD) 3020.40.

How does the DON CIP Team add value to the CNO IVA? The team's approach includes the following activities, categorized by phase.

Pre-Site Visit Research

In addition to coordinating activities with the NCIS Security Training Assistance Assessment Team (STAAT) leader, CIP team pre-assessment actions include:

- Reviewing prior Joint Staff IVA, CNO IVA and other similar reports;
- Soliciting critical CIP-related planning documents, drawings, schematics, etc.;
- Reviewing the installation's assets on the Navy Critical Asset List (CAL);
- Developing a Mission Decomposition Review template of the installation's mission, mission essential tasks and critical assets, which provides a tool that links these items to supporting infrastructure networks; and
- Contacting key installation personnel (public works, security, emergency management, commanding officer (CO) and senior staff) and commercial service providers to set up interviews.

On-Site Evaluation

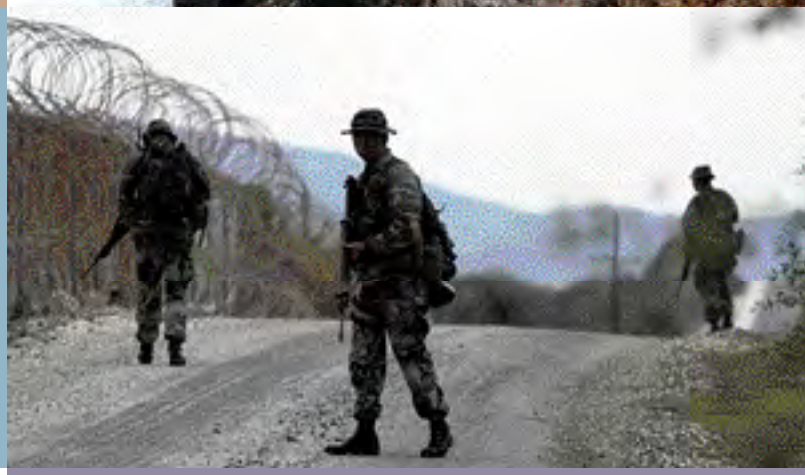
The team tailors the assessment to the installation's mission essential tasks, local geography and key utility services. Once on-site, following a "windshield tour," primary activities include:

- Using DCIP benchmarks as guidance during visual inspections of critical areas and for conducting interviews with key installation participants and commercial service representatives;
- Reviewing Installation Critical Assets with the CO and updating the list as appropriate;
- Validating/updating Mission Decomposition Template with the CO and senior staff;
- Photographing critical assets and plotting with GPS;
- Supporting Consequence Management Planning assessment actions;
- Collaborating with the NCIS team each evening at a "hot wash" of the day's findings;
- Participating in final out-brief of findings to the CO and senior staff; and
- Providing information on another DON CIP initiative: the "Command Remediation Visit" and its Analysis, Strategy and Action Plan (ASAP) Course. (See CHIPS January-March 2007 at http://www.chips.navy.mil/archives/07_jan/web_pages/CIP.html for more information.)

Post-Assessment Analysis/Reporting

Once the assessment is complete, post-assessment activities include:

- Providing the DCIP assessment report to NCIS for incorporation into a final report;
- Recommending updates to the Navy CAL based on findings;
- Updating photo files and latitude and longitude data of the installation's critical assets; and
- Collaborating on a specific plan of action based on the assessment's findings, if the command is interested in remediation assistance.



Photos of Guantanamo Bay, Cuba, shown above.

Waves crash against the southern coastline of Naval Station Guantanamo Bay, Cuba, just east of the base lighthouse July 8, 2005. U.S. Navy photo by Photographer's Mate 1st Class Terry Matlock.

Weapons Company 3rd Battalion, 6th Marines, 2nd Marine Division patrols the fence line in Guantanamo Bay, Cuba, Sept. 10, 2003. U.S. Navy photo by Journalist Seaman Eric L. Beauregard.

A Value-Added Evolution

The CIP team's collaboration with NCIS directly supports the DCIP objective of ensuring consistent, thorough assessments of supporting infrastructure networks in a manner complementary to other DoD programs and efforts, such as: force protection; antiterrorism; information assurance; continuity of operations; Chemical, Biological, Radiological, Nuclear, and High Yield Explosive (CBRNE); readiness; and installation preparedness.

This evolution of DON CIP vulnerability assessment support not only utilizes skills gained from years of NIVA experience, it also enables the completion of a greater number of DCIP assessments on critical DON entities and assets, enhancing CIP posture throughout the DON and contributing to the DoD's efforts for warfighter mission assurance.

For more information go to the DON CIO Web site and click on the Projects Teams tab for the Critical Infrastructure Protection link. CHIPS

For a copy of DoDD 3020.40, Defense Critical Infrastructure Program, go to the Defense Technical Information Web site at http://www.dtic.mil/whs/directives/corres/dir1.html.

DON CIO Presents Excellence Awards at its Successful IM and IT Conference

Department of the Navy teams and projects receive recognition for superior products that assist in the transformation of the Navy and Marine Corps through information technology ...

The winter Department of the Navy (DON) Information Management (IM) and Information Technology (IT) Conference, led by the DON Chief Information Officer (CIO), was held from January 30 to February 2, 2007, at the San Diego Convention Center.

The conference location and timing leveraged the San Diego fleet concentration area and an established conference held at the same time, West, co-sponsored by the U.S. Naval Institute and AFCEA International.

The conference provided a venue to share information about policy, initiatives, and the latest technology related to IM and IT in the DON. There were more than 40 sessions on topics that ranged from service oriented architecture to the civilian IM/IT workforce.

Another DON IM and IT Conference, with a similar range of topics, will be held on the East Coast June 18-21 at the Virginia Beach Convention Center, Virginia Beach, Va. *(For additional information about the East Coast conference, see the announcement on the back cover of CHIPS.)*

A highlight of the conference was the presentation of the DON IM/IT Excellence Awards. These awards are the successor to the DON eGov Awards, which have been presented since 2000, and recognize the superior quality of projects, teams and individuals helping to transform the Navy and Marine Corps through IT.

The awards were presented during a ceremony on the evening of Jan. 31. The award winners received a plaque to commemorate their accomplishments, presented by Mr. John Lussier, the acting DON CIO, and Mr. Dave Wennergren, the former DON CIO, who is now the DoD Deputy CIO.

The following are the 2007 DON IM/IT Excellence Award winners.

Cmdr. Mark Bodoh and Lt. Cmdr. William Batson transformed the way Navy Reservists reschedule and request additional drill periods. Through a streamlined process and supporting Web application, the availability and flexibility of Reservists to provide operational support is greatly enhanced. More than 9,000 manhours were saved as a result of the Real Time Administration of Reservists (RTAR) program during fiscal year 2006.

The Naval Special Warfare Command (NSW) Knowledge Management Working Group implemented KM transformation throughout the command. The NSW KM Working Group created a collaborative environment to promote knowledge sharing, significantly improving organizational efficiency and effectiveness and accelerating the command's migration to Web-enablement.

The FORCEnet Innovation and Research Enterprise (FIRE) team of the Information Sciences Department, Naval Postgraduate School, Monterey, Calif., advanced the Navy's management of knowledge and effectiveness of decision making. The team developed an advanced capability to manage the execution and analyses of complex experimentation in the Navy and Department of Defense. *(See page 40 for more information.)*

Lt. Cmdr. William Batson and Cmdr. Mark Bodoh receiving a DON IM/IT 2007 Excellence Award from acting DON CIO John Lussier and former DON CIO and DoD Deputy CIO Dave Wennergren (right).

The Naval Special Warfare Command (NSW) Knowledge Management Working Group receiving a DON IM/IT 2007 Excellence Award from John Lussier and Dave Wennergren (right). Top row: Jay Washabaugh, Jerry Moy, Bob Hutchinson, Gary Tingley and Joe Aquiningoc. Bottom row: Richard Stakelum, Susan Gross and Conrad Delenia.

The Marine Corps' Manpower Information Systems Support Activity, Kansas City, Mo., and its Manpower Information Systems Support Offices designed, developed, and implemented the Manpower Information Portal. This project ushered in advances in manpower information presentation, management, and access and consolidated over 12 disparate systems, which led to a more secure and authoritative access point for all manpower-related information.

The Navy Cyber Defense Operations Command Prometheus Team developed the primary system used by cyber warriors at

Headquarters Marine Corps Manpower Information Portal team members, Maj. Rob Guice, Lt. Col. Mike Perry, Matt Thompson, Paul Bennett and Ihab Rida, receiving a DON IM/IT 2007 Excellence Award from John Lussier and Dave Wennergren (right).

NCDOC to provide situational awareness of the Navy component of the Global Information Grid. The team used innovative techniques to fuse disparate data elements from myriad sensors to create a holistic system that aggregates, correlates, processes and displays an integrated picture.

The U.S. Marine Corps Traumatic Injury Protection Program (T-SGLI), developed and implemented the Marine Corps' T-SGLI Office. T-SGLI provides monetary assistance to help service members, who suffer a loss as a result of a serious traumatic injury, and their families through the rehabilitation period. Through the effective use of IT, T-SGLI processed more than 1,350 applications and provided eligible Marines with more than $52 million in benefits.

CHIPS

Navy Cyber Defense Operations Command Prometheus team member Jim Granger receiving a DON IM/IT 2007 Excellence Award from John Lussier and Dave Wennergren (right).

U.S. Marine Corps Traumatic Injury Protection Program team members, Lt. Col. Will Goldschmidt, Matt Thompson, Maj. Dan Boersma and Paul Bennett, receiving a DON IM/IT 2007 Excellence Award from John Lussier and Dave Wennergren (right).

Wennergren and Lussier Recipients of Federal 100 Award

Federal Computer Week magazine presents the Federal 100 Awards each year to top executives from government, industry and academia that had the greatest impact on the government information systems community for the previous year. The winners' accomplishments were recognized in the March 26th issue of Federal Computer Week magazine.

The Department of the Navy is proud to announce that John Lussier, acting DON Chief Information Officer, was recognized with a Federal 100 Award for guiding the development of Navy policies for telecommunications, spectrum management, wireless communications and enterprise software initiatives. He initiated a telecommunications cost-recovery audit that identified cases of contract noncompliance, double billing and recoverable taxes.

Department of Defense Deputy CIO David Wennergren and former DON CIO, was recognized with a Federal 100 Award for leading DoD's identity protection and management Senior Coordinating Group, which oversees DoD's smart card, biometric and public-key infrastructure initiatives. He made communication and collaboration a key aspect of implementing DoD's smart card program, even before the federal government undertook a similar governmentwide program under the mandate of Homeland Security Presidential Directive 12.

Wennergren also received the prestigious Eagle Award presented by Federal Computer Week. Eagle awards are given annually to one government official and one industry executive for outstanding contributions to the federal IT community.

The 2007 awards were presented at a black-tie gala March 26, 2007, at the Ritz-Carlton Hotel in McLean, Va.

CHIPS

Spotlight on Excellence

By Barbara Honegger, Senior Military Affairs Journalist
Naval Postgraduate School

The Naval Postgraduate School FORCEnet Innovation and Research Enterprise (FIRE) team received a Department of the Navy Information Management (IM) and Information Technology (IT) Excellence Award for 2007 at the DON IM and IT Conference, hosted by the DON Chief Information Officer.

The award was presented on Jan. 31 to Shelley Gallup Jr., NPS associate research professor of information sciences, the team's experimentation and analysis project lead, by the Deputy Assistant Secretary of Defense for Information Management and Technology and Deputy DoD CIO Dave Wennergren and acting DON CIO John Lussier.

FIRE is a groundbreaking collaborative Web portal supporting knowledge management (KM) and decision making for real-time planning, execution, analysis and reporting of large-scale Navy and DoD experiments. The partially automated enterprise system uses non-proprietary off-the-shelf software and hardware to provide accurate, secure and assured information to authorized Navy, DoD and coalition users worldwide, including those at sea. Web-enabled users anywhere in the world can log on, see the database and graphics, and participate in collaborative decisions.

The award citation reads: "The Naval Postgraduate School's FORCEnet Innovation and Research Enterprise team has significantly advanced the Navy's management of knowledge and effectiveness of decision making in large-scale experiments, such as the Naval Network Warfare Command (NNWC) Trident Warrior series, the Navy's premier FORCEnet sea trial…".

"It was a great thrill for me personally to receive this award on behalf of our group," said Gallup, a former surface warfare officer and 1986 NPS graduate in space systems operations. "It shows that a very small group working hard to produce useful, reliable results can have a very large impact."

According to Gallup, stacks of nominations were received, but Lussier, the acting DON CIO, said that FIRE clearly stood out on top. Gallup also noted the central role that NPS played in Navy experimentation.

"For eight years NPS has played a key role with the Navy in planning, analyzing and reporting on the technology, tactics, techniques and procedures in large-scale naval experiments, and throughout the conference many of the people we've worked with in past experiments had all heard of our FIRE efforts, which means the word has carried very far," Gallup said.

FIRE is the first Oracle enterprise application to work on the Navy Marine Corps Intranet, NIPRNET and SIPRNET, and non-NMCI networks.

"The secret to FIRE's success is exploiting the best of the best database, portal and collaborative software to provide a rigorous structure that forces people to do certain things in a certain sequence in a certain way that ensures the experimentation process is well-planned, well-executed and well-reported," said knowledge management team co-leader and research associate professor of information sciences Randy Maule, the key technical expert implementing the system's architectural vision.

Shelley Gallup Jr. receives a DON IM and IT Excellence Award from acting DON CIO John Lussier, and Deputy Assistant Secretary for Defense for Information Management and Technology and Deputy DoD CIO Dave Wennergren.

"The big change with FIRE is that what started out as physical note pads, lots of phone calls and travel evolved into a real-time collaborative system accessible to anyone with access anywhere in the world," Maule said.

According to Gallup, the history of large-scale naval experimentation management can be divided into "before FIRE" and "after FIRE."

"Before FIRE, constructing the goals, design, execution, data collection, results analysis and documentation of complex experiments was exceedingly manpower intensive and time consuming, because there was no set structure and little or no automation."

FIRE uses a seamless, comprehensive methodology to provide a single authoritative structure that makes the experiment management, data collection, analysis and report development faster and easier with far fewer personnel because everything is done via the Internet. The system significantly increases participation and shared understanding among as many as 200 planners, and the results of analyses are now available in half the time that they were before.

"To date, FIRE has contributed to moving experimentation of new technologies, such as ship-to-ship laser communications, closer to becoming programs of record, as well as transitioning programs of record such as Automated Digital Network System and Common Chat Line, a real-time translation tool, into fleet acquisitions," Gallup said. "Also, the Rapid Technology Transition acquisition cycle has become truly rapid, cut by about 75 percent, down to two to three years."

In addition to Gallup and Maule, the other members of the award-winning team are senior mentor and KM team co-leader Professor Emeritus and former physics department chairman Gordon Schacher; senior mentor and technical writer retired Navy Capt. Jack Jensen; database software developers, information sciences research faculty member Bryan McClain and research associate Diane Smith; associate professor of information sciences Bill Roeting; and data analysis assistant Sharon Prichard. Naval Surface Warfare Center Corona, Navy Reserve teams,

and the Pacific Science & Engineering Group Inc. also provided experts for research and experimentation.

"Gordon Schacher is really the prime mover behind FIRE," Maule said. "He was the original director of the NPS Institute for Joint Warfare Analysis where this experimentation innovation began." CHIPS

2008 DON IM/IT Excellence Awards

The call for nominations for the 2008 Department of the Navy Information Management/Information Technology (IM/IT) Excellence Awards will be announced by a DON Info Alert (electronic newsletter) and naval message in fall 2007. The purpose of these awards is to recognize superior quality of IM/IT projects, teams and individuals helping to transform the Navy and Marine Corps through information technology.

DON teams and individuals of all ranks, rates and grades are eligible to apply for an award. A combination of team and individual awards will be presented. Team awards will be presented to project teams, process/product teams and working groups. The team must include government civilian or military employees, but may include contractor personnel as well. Representation from the other services on joint projects involving the DON is welcome. Individual awards will be presented to government civilian or military employees.

Individuals and teams that meet one or more of the following criteria will be considered for an award:

- Superior leadership skills, delivering results that ensure the organization is working toward common solutions, and aligned to the DON IM and IT strategic vision (as defined in the DON IM and IT Strategic Plan for FY 2006-2007 available at http://www.doncio.navy.mil);
- Innovative use of IM/IT while not duplicating existing projects, systems or solutions;
- Significantly improving the efficiency and effectiveness of the organization in delivering its mission;
- Significant achievement in advancing the DON's vision to manage knowledge to enable effective decision-making, increase the efficiency of task accomplishment and improve mission effectiveness;
- Significant contributions that enable information assurance or critical infrastructure improvements;
- Significant contributions to the recruitment, retention, and training of the IM/IT workforce.

Awards will be presented during the DON IM and IT Conference scheduled for Feb. 4-7, 2008, at the San Diego Convention Center, 111 West Harbor Drive, San Diego, Calif.

To sign up for the Info Alert and receive the 2008 call for nominations, go to the DON CIO Web site at http://www.doncio.navy.mil, click on Info Alerts and News on the left side of the screen, or call (703) 602-6274 for more information. Details about the conference will be announced in the coming months in CHIPS and by a DON Info Alert. CHIPS

Last Known Yeoman (F) Laid To Rest

By Sophie Platt, Naval Historical Center Public Affairs

Charlotte Louise Berry Winters, the last known Navy Yeoman (F) and woman veteran of World War I, was laid to rest March 30 in Frederick, Md. Winters died at the age of 109 on March 27. Her funeral was attended by an honor guard, pall bearers, and firing party from the Navy Ceremonial Guard, along with family and friends.

Vice Adm. Nancy E. Brown, Joint Staff director for Command, Control, Communications and Computer (C4) Systems, presented the casket flag to the family.

After enlisting in 1917, Winters served at the Washington Navy Yard in Building 57, current home of the Naval Historical Center. One of the last Yeoman (F)s to be discharged in 1919, she was immediately hired by the Navy as a civilian employee to fill her active-duty job.

"Ms. Winters was a trailblazer, one of a relatively small group of women to serve in our Navy during World War I. She did so honorably and nobly, helping through that service to bring freedom to millions of people all across Europe and hope to thousands of young women all across America," said Chief of Naval Operations Adm. Mike Mullen.

"She and her shipmates answered the call when the nation needed them most. They worked hard. They struggled. They persevered, and they set a shining example. And, as in Ms. Winter's case, some stayed on to prepare the Navy to fight and win yet another World War. They were patriots, and we will remain forever in their debt," Mullen added.

Winters was a founding member of the National Yeoman (F) veterans' organization, and served as its eighth commander from 1940-1941.

The Yeoman (F)s, popularly called 'Yeomanettes' to their objection, were established by Secretary of the Navy Josephus Daniels in 1917 after the U.S. entry into the war.

At the time the Navy and Marines were the only branches of the U.S. armed forces to enlist women to serve in a similar status with men. The expanding Navy and Marines had a dire need for more clerks and stenographers, while also needing to free male Sailors and Marines for fleet duty. Recruited at first just for clerical duties, by the end of the war their jobs included language translators and munitions workers in factories.

Records show that 11,000 Yeoman (F)s, 1,713 female nurses and 269 women Marines (Marinettes) served in World War I. For many years they, along with Army nurses, were the only women eligible to join the American Legion, and the only ones eligible to receive a bonus voted to veterans of World War I.

The Yeoman (F)s were of such invaluable service to the country that there was no question of women returning to Navy service during World War II as the WAVES (Women Accepted for Voluntary Emergency Service).

The success of the WAVES in turn paved the way for the 1948 permanent establishment of women in the Navy. So, not only did the Yeoman (F)s provide exceptional service during World War I, they set a standard of excellence for women in the U.S. military which is carried on today.

The Naval Historical Center has more information on the "Yeomanettes" at http://www.history.navy.mil/photos/prs-tpic/females/yeoman-f.htm. For more news from the Naval Historical Center visit http://www.news.navy.mil/local/navhist/.

This article has been edited from the original which appeared on Navy NewsStand March 30, 2007. Go to Navy NewsStand at http://www.navy.mil for more news from around the fleet. CHIPS

Introduction

The United States Navy is embarking on an ambitious initiative to craft a new maritime strategy. This will be the first new Navy strategy in a quarter-century, and the first one that addresses the post-Cold War and post-9/11 realities of the global war on terror. The Chief of Naval Operations Adm. Mike Mullen has indicated that this new strategy will be consistent with the National Security Strategy and the National Strategy for Maritime Security, as well as with other national level guidance.

As a key part of this strategy, Adm. Mullen has made the Global Maritime Partnership *(originally titled the 1000-ship Navy)* a key tenet of U.S. naval policy. The CNO has made it clear that he expects the Navy to work seamlessly at sea with a wide range of coalition partners.

This policy is already impacting the requirements generation process for the Navy, with the Deputy Chief of Naval Operations for Communications Networks and Navy Chief Information Officer, Vice Adm. Mark J. Edwards, directing his staff to "ensure coalition interoperability is considered at the earliest stages of capability development."

As the chief operating officer (COO) of the Naval NETWAR FORCEnet Enterprise (NNFE) and commander of the Space and Naval Warfare Systems Command (SPAWAR), Rear Adm. Mike Bachmann, leads the Team SPAWAR effort spearheading the work by the Navy's science, engineering and acquisition community to deliver FORCEnet capability to naval operators to make the Global Maritime Partnership a reality.

Coalition Operations

Coalition operations have become an increasingly important issue within the Navy — not only as a policy issue but as a practical issue for operators at sea. Third Fleet Commander Vice Adm. Barry Costello highlighted this fact during the NNFE and Industry Conference last fall when he said that fleet commanders unanimously identified one issue as their top priority: coalition communications. These commanders know from experience that coalition interoperability is the key to a successful mission.

The Navy's ability to communicate and exchange information with coalition partners is not only vital from a warfighting perspective, but is also integral to a wide array of humanitarian missions around the world. The tsunami relief efforts in December 2004 dramatically brought home the need for effective coalition communications. While coalition members were able to deliver much needed relief supplies, commanding officers were often challenged in communicating and exchanging information with their coalition counterparts. Current and future efforts to bring about the Global Maritime Partnership must address the ongoing challenge of coalition interoperability. Coalition communications will not only enhance the Navy's warfighting capabilities but will also help the Navy meet the growing humanitarian missions that will become part of the new maritime strategy.

Operational Demands, Technical Imperatives

Based on long-standing Team SPAWAR projects, such as the Combined Enterprise Regional Information Exchange System (CENTRIXS), to enhance coalition networking at sea, SPAWAR has the embedded subject matter expertise to take coalition networking at sea to the next level. While there are several efforts along those lines currently underway, The Technical Cooperation Program's "FORCEnet Implications for Coalition Partners" initiative has taken a unique approach to defining coalition networking needs in terms of both immediate and future technologies and functions.

TTCP is a forum for defense science and technology collaboration between Australia, Canada, New Zealand, the United Kingdom and United States. Established as a joint effort between the Defense Department, the Department of Commerce and the respective agencies of the other four nations in the 1950s, TTCP is probably the largest collaborative defense science and technology activity in the world.

The statistics alone give some indication of the scope of this effort: five nations; 11 technology and systems groups formed; 80 technical panels and action groups; 170 organizations; and 1,200 scientists and engineers. By any measure, TTCP is a broad-based effort that tremendously facilitates science and technology cooperation among the five member nations. Importantly, while conducting this sort of interaction in other forums is certainly possible, the extant TTCP organization and infrastructure provide a ready-made medium that has made success in this endeavor probable.

The aim of TTCP is to foster cooperation within the science and technology areas needed for national defense. The purpose is to enhance national defense and reduce costs. To do this, TTCP provides a formal framework that scientists and technologists can use to share information among members. This is a primary reason why Team SPAWAR is involved in this effort.

Collaboration within TTCP provides a means of acquainting the participating nations with each other's defense research and development programs so that each national program may be adjusted and planned in concert with the efforts of the other nations. This process avoids unnecessary duplication among the programs, promotes concerted action and joint research to identify and close important gaps in the collective technology base, and it provides nations with the best technical information available.

TTCP has its center of gravity in the applied research domain, but it also encompasses basic research and technology development activities. The scope includes the exploration of alternative concepts prior to development of specific weapon systems, collaborative research, sharing of data, equipment, material and facilities, joint trials and exercises, and advanced technology demonstrations. Cooperation within TTCP often acts as the catalyst for project-specific collaborations further along the acquisition path.

"FORCEnet is a key enabler for the 1,000-ship Navy. We are embarked upon a journey to ensure that we're interoperable not only with the other services that are critical to our warfighting effort, but also with our allies. We're at the point where we can make this capability available to our trusted allies, and we plan to do that."

– Rear Adm. Michael C. Bachmann
Commander SPAWAR

The FORCEnet Implications for Coalition Partners initiative was assigned to TTCP Maritime Systems Group (MAR), Action Group Six (AG-6), with Team SPAWAR assuming a key role in the leadership of this action group. For the past several years, MAR AG-6 and its predecessor, MAR AG-1, have been involved in analyzing maritime network-centric warfare options for coalitions, and how these options might be implemented in the network procurement programs of each individual nation.

In seeking to establish the basic requirement for the technologies to be included in these options, AG-6 began with a common understanding of the operational environment facing a coalition naval force. The group developed a scenario for a coalition naval force that began as disaster assistance/humanitarian relief, then moved into a counterterrorism effort, and ultimately a high-tempo conflict at sea.

Four principal measures of effectiveness — Time to Capability, Economy of Effort, Risk and Campaign Success — were devised to measure the effectiveness of a robustly networked coalition force that fully leveraged the U.S. Navy's FORCEnet capability compared to one that was not networked.

In addition to the analysis of networked forces versus non-networked forces, AG-6 members liberally shared the "technology on-ramps" of their respective national acquisition communities in order to find the windows where complementary technological capabilities could be inserted into their naval C4ISR, or command, control, communications, computers, intelligence, surveillance and reconnaissance, systems.

By modeling the planned capabilities of these "on ramps" against the scenario, the impacts and value of alternative coalition network structures are being assessed. The resulting analysis will be used by AG-6 members to make specific procurement recommendations in their respective countries. Team SPAWAR is taking the lead sharing this information with the NNFE.

Mr. Don Endicott, head of the Communications and Information Systems Department at SPAWAR Systems Center San Diego, is the AG-6 chairman and has been coordinating the group's efforts for the past several years.

Endicott put a punctuation mark on the group's efforts when he noted that: "While the AG-6 analysis effort spans a wide spectrum of operations from planning through operations other than war, through potential conflict with a capable adversary, our initial findings indicate that one of the greatest benefits of coalition networking at sea may well be our ability to 'virtually train' with our likely coalition partners well in advance and en route to an operation. In this way, when we begin to operate at sea together we will not be in a pickup game."

Dr. Bill Rix and his team in the SPAWAR Office of the Chief Engineer are supporting the AG-6 effort to generate analytical data and conduct modeling and simulation to demonstrate that if FORCEnet is developed in a way that is inclusive of likely coalition partners, who, in turn, build their national systems to be compatible with FORCEnet, the coalition of naval forces involved will enjoy a quantum increase in capability.

According to Dr. Rix, "Current systems and technologies are probably capable of supporting coalition collaboration if all the circumstances are anticipated in advance. Modeling and simulation tools can be brought to bear to determine the improvement in humanitarian operations or warfighting capability achieved in unanticipated scenarios, when coalition partners have invested in common and interoperable systems. This should help coalition and U.S. senior decision-makers to make more informed investment decisions."

Key to Our Future Naval Capability

Team SPAWAR is spearheading the AG-6 effort because an at-sea communications solution with coalition partners is unlikely to be effective, if it is conceived and developed solely in U.S. defense labs, and then inflicted on coalition partners. Inter-laboratory cooperation with these likely coalition nations is the surest way to realize the goal of long-term effective coalition communications at sea. Without this cooperation, effective coalition communications may well remain out of reach.

The nature of this Team SPAWAR-championed effort has attracted a number of organizations outside the SPAWAR naval laboratory and acquisition community. Some of these organizations like the Office of Naval Research, the Naval War College and the Naval Postgraduate School have placed members on this team because they recognize the importance of its work.

In addition to enhancing networking at sea between and among likely coalition partners, this effort has the potential to also help Team SPAWAR and the NNFE provide the analytical underpinning to determine "what a pound of C4ISR is worth."

The importance of coalition networking was the subject of a panel discussion at a recent major defense conference in San Diego. At that event, Bachmann, as a participant in a panel discussion with the Deputy Chief of Naval Operations for Information, Plans and Strategy, Vice Adm. John Morgan, said: "FORCEnet is a key enabler for the 1,000-ship Navy. We are embarked upon a journey to ensure that we're interoperable not only with the other services that are critical to our warfighting effort, but also with our allies. We're at the point where we can make this capability available to our trusted allies, and we plan to do that."

Bachmann's remarks sum up the key role Team SPAWAR plays in providing the technical underpinning and international cooperation — at the science and technology working level — to ensure that the Global Maritime Partnership becomes a reality. The work of the TTCP AG-6 FORCEnet Implications for Coalition Partners is an essential contribution to Team SPAWAR.

George Galdorisi is the director of the Decision Support Group for SPAWAR Systems Center San Diego. He has been working with the TTCP and coalition networking for the past six years.

Dr. Stephanie Hszieh is a strategic analyst in the Decision Support Group and received her Ph.D. in political science from the University of Southern California.

Terry McKearney supports the TTCP's modeling and analysis of network capabilities and requirements.

CHIPS

Senior Pacific Fleet Leadership Pitches Navywide Knowledge Management

By U.S. Pacific Fleet Public Affairs Office

Deputy Chief of Staff for Plans, Policies and Requirements, U.S. Pacific Fleet Rear Adm. Joseph P. Mulloy advocated his support for the Navy to assimilate the Pacific Fleet's (PACFLT) successful electronic knowledge management (eKM) model during a high-level briefing at the Information Management and Information Technology Conference Jan. 30 at the San Diego Convention Center.

Knowledge management is a systematic approach to aligning people, processes and tools to maximize performance for a desired outcome. PACFLT's eKM strategy includes the use of a knowledge portal and an effects-based approach for quantifiable results to ensure knowledge leads to maritime security and the commander's intent. PACFLT is advertising its eKM solution for Navywide use.

"The vision, goals, objectives and strategies of our leadership clearly define what we are expected to do," said Mulloy, who is also PACFLT's chief knowledge officer. "Taking our cue from Navy leadership, we've produced a successful model for fostering and creating an information and knowledge sharing environment that is creating efficiencies and raising effectiveness both within and among adopting organizations."

According to Lt. Cmdr. Tony Bruce, deputy chief knowledge officer, knowledge-based organizations, teams and systems are characterized by the phenomenon known as the network effect — a term that reflects the value and effectiveness of an organization as its user population expands.

"As more and more users join the organization and contribute to it, the body of information and knowledge it comprises grows at an exponential rate making it an increasingly valuable resource," Bruce said. "People in this knowledge-based organization must do more than just be connected in order to share the information and knowledge. They must have a mind-set or belief that encourages and rewards them to participate."

PACFLT's eKM model is an asynchronous-collaboration tool set, which offers a calendar, out-of-office tool and action tracker to aid in workflow and scheduling as well as document storage.

U.S. Pacific Fleet Deputy Chief of Staff for Plans, Policies and Requirements Rear Adm. Joseph P. Mulloy discusses Pacific Fleet's eKM model at the Department of the Navy Information Management and Information Technology Conference Jan. 30 in San Diego, Calif.

Ms. Jamie Hatch, electronic knowledge management specialist, explains the various aspects of eKM to military members and civilian employees during a training session for users at U.S. Pacific Fleet headquarters aboard Pearl Harbor, Hawaii.

"The tools and technology of eKM are simply enablers that act like a catalyst does in a chemical reaction," Mulloy said. "They contribute nothing to the end result of the reaction of two chemicals, which in our case is people and processes, but are essential to make them react and work together."

PACFLT's eKM model also enables global connectivity because it's Web-based and not dependent on the Navy Marine Corps Intranet (NMCI). Users can access eKM from any computer with Internet access and a Common Access Card (CAC) reader. This allows secure access for overseas commands, remote sites and personnel on travel, which is a major advantage of the model.

"The benefit of having a Web-based technical solution is helping the end user's effectiveness by 'sharing in' and accessing a single environment," Bruce said. "The 'IT tail' of such a model is also very efficient and can be scaled to fit the user's needs, Bruce said. "

The importance of scalability is supported by the fact that there are 150 commands using eKM and about 15,000 users, Bruce said.

"The eKM model can be tailored by each command through the use of business rules," Bruce said. "One of the reasons for this is the technical environment tools which are shared across the entire enterprise. The single eKM (database) is critical to eliminating technological stovepipes that have plagued existing network-based enterprises because tools cannot span the entire Navy."

PACFLT is confident eKM can easily integrate into the existing Defense Knowledge Online (DKO), a service gateway offering many of the same benefits as eKM.

"Although we've had no direct contact with anyone associated with DKO to develop a plan, we are positive eKM will easily integrate," said Bruce. "Many commands are already using applications such as SharePoint and Navy Knowledge Online as front ends and have incorporated portions of eKM into their working environment."

"The Pacific Fleet area of responsibility spans 16 time zones from the Panama Canal to the Persian Gulf. We need a system that allows us to link for collaborative planning and action — eKM is that system."

– Rear Adm. Joseph P. Mulloy

Although current bandwidth limitations allow eKM to support only 200,000 users, PACFLT is driven by the prospect to expand eKM availability and has outlined a phased-approach plan to support 600,000 Navy users. This phased-implementation approach would reduce delays and cost, Mulloy said.

"The potential effectiveness of a networked, seamless team of more than 600,000 Navy, Marine Corps, civilian and contractor personnel cannot be underestimated, and eKM provides an opportunity to make this dream a reality," Mulloy said.

Both the Unclassified but Sensitive Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) networks support eKM operations. Sharing information on both sites is controlled by community membership, which can be as large as an entire command or as small as one individual. Community membership also adds to the security of eKM.

"In addition to the standard security measures everyone must have to access a Department of the Navy network, the sharing of information on our NIPR and SIPR sites is controlled by community membership," Bruce said. "While membership size of a community may vary, who has access to the community is always controlled."

"The Pacific Fleet area of responsibility spans 16 time zones from the Panama Canal to the Persian Gulf," Mulloy said. "We need a system that allows us to link for collaborative planning and action — eKM is that system."

Enabled by senior PACFLT leadership's full commitment and supported with the education and guidance of proven change management and process improvement teams, a culture of sharing, collaboration and efficiency has begun across the entire area of responsibility.

For more information visit the Pacific Fleet on the Web at http://www.cpf.navy.mil. CHIPS

NPDC Names Recipients of First Knowledge Management Awards

By MC1 (SW/AW) John Osborne, Naval Personnel Development Command Public Affairs

The Naval Personnel Development Command (NPDC) held its first Knowledge Management Awards Board in January and the winners were announced by Rear Adm. Moira Flanders, commander, NPDC, during the most recent Commanding Officer/Command Master Chief Conference in Pensacola, Fla.

Knowledge management initiatives began at NPDC four and half years ago, and today, KM has become the process by which leadership utilizes the training tools at their disposal to effectively manage corporate knowledge in their commands.

The awards were given in the categories of Community of Practice (CoP) and Innovation. Master Chief Legalman (SW) Donna Sayers from the Center for Service Support (CSS) Athens, Ga., took home the CoP Award.

Sayers' award was based on her development and management of a CoP on Navy Knowledge Online (NKO) that enables collaboration and knowledge sharing across the legalman community. Sayers said her goal in building the CoP was to provide LNs with standardized training, reachback points of contacts, and direct links to the forms and directives they need to perform day-to-day duties. She also wanted a knowledge portal that could keep information current and be as readily available to LNs on independent duty or serving in remote locations as it is to those serving in Navy Legal Service Offices where they have at least one chief petty officer and an experienced LN available.

"I think one of the big differences in the LN CoP is [that] although it provides training, its focus is not only on training," said Sayers, whose CoP can be accessed through NKO at https://www.nko.navy.mil.

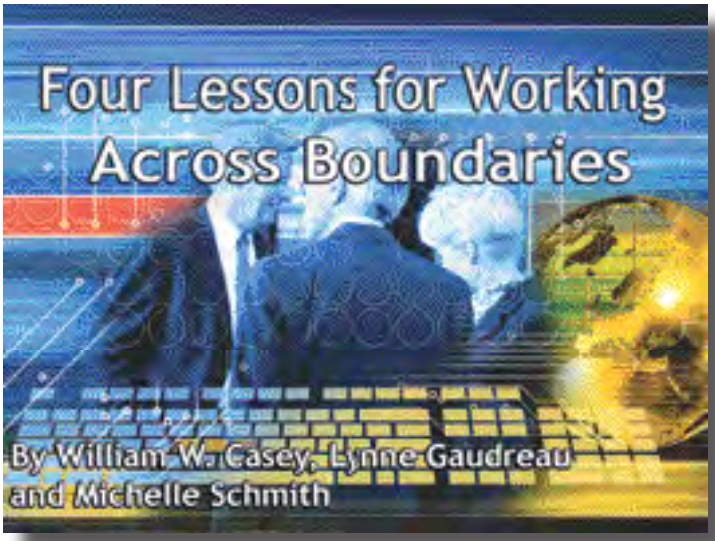
The Innovation Award was split between Mass Communications Specialist 1st Class (SW/AW) Jorge Morales from CSS and Fire Controlman 1st Class (SW) Christopher Downing, Fire Controlman 1st Class (SW) Daniel Mohn, Electronics Technician 2nd Class (SW) Francisco Noguera, Mr. Peter Shepherd and Mr. Timothy White, all from the Center for Surface Combat Systems, Great Lakes, Ill.

CSS is one of 16 Learning Centers, and CSCS Great Lakes is one of more than 60 learning sites aligned under NPDC, which is responsible for providing Sailors with the tools, knowledge and opportunities for their personal growth and professional development.

"The Center for Service Support and Center for Surface Combat Systems have displayed excellence both in building a community base of collaboration that helps people learn from one another more efficiently, and they have excelled at developing innovations that help make the Navy more mission capable and ready," said Jon Harris, knowledge manager for NPDC, who is responsible for the development and implementation of the knowledge management strategy for the NPDC domain.

The CoPs for ETs or FCs can be accessed by logging into NKO at https://www.nko.navy.mil, and entering the appropriate directory name for each rate in the search bar. CHIPS

ET2(SW) Francisco Noguera, Mr. Timothy White, Mr. Peter Shepherd, FC1 (SW) Christopher Downing and FC1 (SW) Daniel Mohn from the Center for Surface Combat Systems, Great Lakes, Ill., were recognized for innovative training concepts with the first Community of Practice and Innovation Award from Naval Personnel Development Command.



The Policy Challenge

Getting large organizations in sync when it comes to publishing and implementing policies and procedures can be a challenge. For one thing the policy developer and implementer often are not in the same department. As a result, implementation of the policy is carried out by people who do not work for the developer. The implementer and developer may be mandated to work in different directions, thereby creating and maintaining their own "silos" within the organization.

How do you reach across the structure of a large organization and get different departments to cooperate? This question is so common throughout large corporations and government agencies that when a policy-making group finds the solution, it is worth paying attention to. There may be valuable lessons to learn, such as how to promote understanding and teamwork.

Four Lessons Learned, So Far

The Department of the Navy (DON) Information Management (IM) and Information Technology (IT) Performance Measurement Program is just such an example of how the DON Chief Information Officer (CIO) staff met these challenges head on and learned how to work across boundaries. The objective of the program is to align command-level IM/IT goals with DON enterprise level IM/IT goals; in other words, to get everyone to follow the DON IM/IT Strategic Plan, and to do it using a common set of metrics by which progress will be assessed. This is an important and ambitious plan that promotes interoperability, security, and more. But the challenge is the actual execution of the plan, knowing that each organization has its own priorities, pressures, constraints and history.

In the DON, big steps were taken in seemingly simple ways, with impressive interim results: Diverse personalities and groups are now sharing information across boundaries for the common good. For a large government organization, this is not an easy accomplishment. While it may sound right and obvious, it does not reflect natural human tendencies, particularly in large organizations. The ultimate goal of the program still lies ahead, but progress is steady and early returns suggest a very favorable prognosis. Here are four lessons from that effort, so far.

Lesson #1: Practice What You Preach

Before asking anyone else to align metrics to strategy, DON CIO personnel did it themselves. Though a deceptively simple idea, "modeling what works" is a remarkably effective method to encourage people to adopt new behavior. Starting with then CIO, Dave Wennergren, the DON CIO articulated its own piece of the DON IM/IT strategy as a set of measurable results or "effects" and then cascaded these effects down to the level of individual accountability. "Lead by example" has been Wennergren's mantra, and it seems to be working for him because he was recently promoted to be the Department of Defense Deputy CIO!

This internal alignment has resulted in at least three positive outcomes. It has: (1) ensured that staff energy is focused on those activities that support the DON IM and IT Strategic Plan; (2) provided the foundation for the SMART Objectives to support the National Security Personnel System; and (3) created a common understanding of how success will be measured.

In addition, tools were developed to assist the DON CIO's continued focus and provide a mechanism by which teams are able to demonstrate progress.

The Whole Goal (WG) Alignment Map is the high level document that captures the results or WGs for each team and shows their alignment to the goals of the DON Deputy CIO (tier 2 level goals) and the goals of the CIO (tier 1); the Master Task List is a Microsoft Project-based tool that defines the key tasks and associated time lines teams have identified as critical to the achievement of WGs; and the DON CIO Internal Dashboard provides a simple graphical representation of actual progress.

DON CIO also followed the dictum, "Do good and avoid evil." This is a reference to the Whole Goal concept, an important idea taught by the Naval Postgraduate School in the Navy's Executive Business and Corporate Business courses.

By "Whole Goal" we mean that each effect was encapsulated as a single measurable desired effect to achieve with measurable negative side effects to avoid. Steering clear of unintended consequences is integral to the Whole Goal approach.

DON CIO leaders now gauge progress against measurable Whole Goals and ensure ongoing strategic focus through periodic "effects-based assessments" with their teams. In those meetings, teams tweak strategy, target issues to resolve and reinforce goal achievement.

It is this successful internal alignment and performance measurement effort that led to DON CIO's broader initiative to establish an IM/IT Performance Measurement Program to assess and report Department-wide progress toward the achievement of its IM/IT strategic goals.

Lesson #2: Be Focused on Your Result, But Flexible

The approach of the DON IM/IT Performance Measurement Program is to collect metrics from across the Navy and Marine Corps that are relevant to the execution of the DON IM/IT Strategic Plan, and then to create a one-stop-shopping dashboard made easily accessible to all concerned parties. The dashboard, developed by the DON CIO, provides a way for the Department's commands and organizations to compare themselves and each other against agreed upon goals and measure progress.

That's the blueprint, but there is a temptation simply to cobble together any and all available metrics. This is common practice in "metrics" efforts. The DON CIO could have collected a vast quantity of metrics whose resemblance to the strategic plan, if any, was purely coincidental.

But that is not what happened. The DON CIO asked for and received only metrics relevant to the Strategic Plan. However, even while being selective in the metrics employed, the pervading tone has been one of respect and collaboration. Ever mindful of project milestones, the team, nonetheless, invested heavily in the time it takes to build trust. The attitude — one that says we are open to learning and to new ideas and methods of doing things — invited trust and partnership. This is one aspect of the project that we hope others will notice; it is a key to inspiring good ideas and cooperation, and a catapult to future successes.

Lesson #3: Promote a Common Language

Any program dashboard is meaningless unless apples are being compared to apples, but escaping the "Tower of Babble" is difficult. Different organizations use different words for the same things and the same words for different things. For example, what one organization considers to be a single "legacy system," one that is old and difficult to support, may be considered by another organization to be three legacy systems, and yet another organization might not consider it a legacy system at all.

Sorting out common terms and meanings takes effort. It often means that at the beginning there will be disagreements and drawn-out discussions, but as difficult and inconvenient as that can seem, it is crucial for the success of any cross-functional effort, especially those entailing measurement.

The DON CIO Performance Leadership and Management Team tackled this problem through consensus. Getting everyone to use the same language and definitions took an incremental and iterative approach that was worth every minute invested, especially in gaining ideas, input and buy-in from the Navy and Marine Corps' IM/IT gurus and experts within the DON CIO. These discussions evolved into a "metric definition template," a straightforward format for describing candidate metrics, defining data owners and capturing data collection methods.

Another key to common language has been the team's investment in education early on. Through briefings and one-on-one communication, all DON CIO staff members and core DON IM/IT stakeholders became well-versed in the DON IM/IT Strategic Plan, the characteristics of good metrics and the goals of the performance measurement initiative itself. When people begin an initiative with a common understanding of direction and principles, consensus comes more easily.

As important as the early investment in education has been to this initiative, perhaps the greater lesson learned is the recognition that this promotion of common language is a continuous education requirement. Key players change, and the collective understanding of what is useful evolves as the effort matures. The continuous education, information sharing, consensus building and documentation of key definitions and business rules are critical to ongoing success. A metrics template proved to be an invaluable tool in structuring these discussions and documenting final agreement for defined metrics.

Lesson #4: Don't Get Fancy

The program team is using tried and true Web tools and Excel spreadsheets to accomplish what they need to. The dashboard is hard to break and easy to pay for. It's simple. It works.

Just like the temptation to get tangled in metrics, getting hung up on expensive, high-powered technology is also widespread and limiting. Later, if funding becomes available, upgrading to less manual and more powerful processes is a possibility. Meanwhile, the team is not beholden to vendors, funding agents or technological grandiosity.

Likewise the program team's project plan is hewed to simplicity. Leaning heavily on realistic goals and time frames, iterative efforts and consensus-building, the entire effort has been an exercise in the art of the possible.

It's Not Over

It has been just over six months since this program launched, so there is still plenty to be done. For example, the entire DON IM/IT Strategic Plan is not yet fully reflected in the metrics, even though all the metrics supplied so far do relate to the plan. Adding to the challenge is the fact that the DON IM/IT Strategic Plan is a moving target, updated and released every two years. So a complete reflection of the plan is still to come, and will continue to depend on collaborative relationships across naval organizations.

Will these metrics become goals and the goals become accountabilities? After all, that's how one advances a strategic plan. That decision will be up to the individual commands, but we think the answer is yes. Meanwhile, this program will have created a common language, a common dashboard and a common standard — all rooted in the DON IM/IT Strategic Plan.

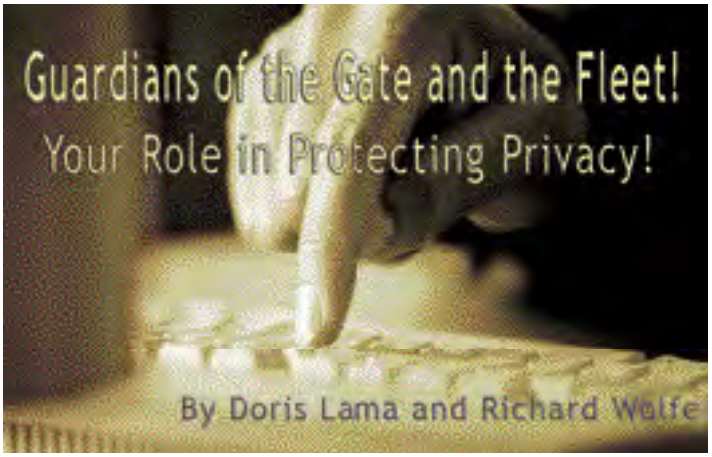
A Good Example

Given human inclinations, this example of a group able to thoughtfully choose relevant metrics and share information and goals, should push others to achieve something similar or even better. In fact, Army and Air Force CIO organizations have already expressed interest in using this approach as a model to address their own parallel goals. But the implications are broader, still.

This is a standard for large organizations working together to join hands at the "seams," and produce the right result. It is an efficient use of limited resources, and an effective use of what we have in unlimited amounts – imagination, ingenuity and the capacity to see big goals — and how we each can make sure these goals are met.

Oh, the Places You'll Go! — this Dr. Suess story reminds us of the experiences of those involved in this program. It cleverly celebrates joys, challenges and even disappointments on a journey. Unknown territory, confusion and criticism are experienced, but ultimately, mountains are moved and success is obtained!

Led by Michelle Schmith, the DON CIO Performance Leadership and Management Team is comprised of William Casey, Lynne Gaudreau, Michael Khalifeh, James Kopetsky and Darlene Greifenberger. The team's Navy partner is N6, Deputy Chief of Naval Operations for Communications, represented by Harry McDavid and Denzil Thies. The team's Marine Corps partner is Headquarters Marine Corps C4I, represented by Robin Thomas and Brad Ellis. CHIPS



Consider this scenario: a major university in the Eastern United States finds that its Naval Reserve Officer Training Corps information site is hacked. Important private information pertaining to enrollees is stolen. The information is posted to a popular Web site and exposed to a huge audience. The hacker also posts how it was done and invites others to duplicate the theft at their institutions. Sound like a science fiction tale? No, it really happened not too long ago!

Many federal agencies have had the misfortune of reporting the loss of personally identifiable information (PII)— information that pertains to individuals, such as their name, Social Security Number (SSN), salary, and more. Recently, one breach involved the theft of 1.3 million medical records!

Here are a few more breaches that have recently occurred:

- A Navy recruiting station reported that 31,000 individuals were impacted when two legacy laptops were stolen from its office.
- A Naval Hospital Corps School reported that 60 to 70 students were impacted when a portable data storage device was stolen along with other personal effects from an office desk drawer during normal working hours.
- A command career counselor reported that 117 Selected Reservists were impacted when his car, which contained both a laptop and thumb drive containing personnel information, was stolen.

Your Help is Needed!

The Department of the Navy (DON) needs your help in protecting private information — your own and your teammates'! Personal information breaches cost money, which is not budgeted; time to perform a myriad of administrative functions; frustration — because you will have to explain what happened; and embarrassment — to you and your organization because it happened on your watch.

The purpose of this article is to ask you to factor in privacy safeguards as you do your job. Think about your role in this effort. When you came into the government as a civilian or contractor employee, or joined the military, you knew that as a condition of your employment you would need to provide personal information about yourself.

If you were appointed to a high level position, you were required to share financial information; if you required a security clearance, you had to provide lots of personal information — much more than just the basic name, SSN and date of birth. The form contained a Privacy Act Statement to tell you why the information was needed, and it implied that every step would be taken to protect your personal information from unauthorized disclosure.

But as you know, the world we live in is changing fast! Information flow is easier and faster. Paper records have morphed into electronic records, and what used to take time to disseminate can now be done in an instant with the push of a button. Thumb drives have replaced floppy disks and personal information is stored in many forms.

Recent e-government mandates require transparency of privacy programs. The federal government is committed to the goal of having its citizens understand what private information is collected and how that information is used. At the same time, the government wants federal employees to ensure that safeguards are deployed to protect personal information.

The DON has been fortunate to team with the Naval Audit Service, which also seeks to ensure that the Department adopts and adheres to best privacy practices. During recent audits, auditors found that DON recycling bins and waste containers were filled with papers containing personally identifiable information, seemingly without a thought about better protecting this data. Some people mistakenly think that the recycler is responsible for shredding or burning these documents. But the reality is — they are not. We, the users, are responsible, and we must be vigilant in the handling of personal information!

Policy Guidance

The Office of Management and Budget, the policy official for the Privacy Act, has been working on a new notification requirement since the report of the Department of Veterans Affairs security breach involving 27 million veterans in 2006. OMB is working with agencies to bring a halt to breaches by establishing new business practices to protect privacy.

OMB is considering holding employees accountable when their actions result in the loss of PII. In the future, the lack of attention to the secure use, storage and disposal of private information may result in punitive action. Just imagine having a stellar career change in an instant — as a result of a security breach that costs you your job or a promotion!

It is apparent that we have come to rely on the Social Security Number as the primary identifier. But the Social Security Administration states that this was not its intended use. While it is evident that a change is needed, it will take time and money to retool federal IT systems to remove the SSN as a personal identifier.

While agencies are currently providing comments on recommendations regarding use of a different identifier, the bottom line is that the cost of breaches on all levels — monetary, embarrassment, and risk to privacy and identity theft — is too high. Agencies will be required to take aggressive steps to eliminate the potential for breaches of PII.

The solution to eliminating breaches begins with you! Why? Because you use, disseminate, collect, and manage great amounts of personal information, and it is your diligence that will enable the DON to minimize loss of PII.

Alerting DON personnel to their role and responsibility in protecting privacy is key to minimizing and possibly eliminating breaches. To this end, the DON has had privacy standdown

training and developed training materials, ads, plan of the day notes, and other tools to get the word out. Most can be downloaded from the DON Privacy Office Web site at http://privacy.navy.mil.

In the DON, more than 220 Navy and Marine Corps systems contain personally identifiable information, which is retrieved by an individual's name and personal identifier. For these systems, the DON is performing Privacy Impact Assessments, a tool originally developed by the Internal Revenue Service to ensure the integrity and safety of the myriad of documents containing personal information that it receives to compute taxes.

The Department asks you to ensure that breaches are eliminated and privacy is protected by following sound business practices to protect PII, including:

- Be sure to secure! Make sure documents containing PII are not accessible to compromise or loss.
- Encrypt, Encrypt, Encrypt! When transmitting data, make sure that you use a secure connection. If you don't know how to do it, find out soon. The procedure is easily learned.
- If you don't need the information, don't take it with you — electronically or on paper!
- Once you have read it, shred it! Don't let it stack up on you.
- Browse the World Wide Web smartly! Make sure that your security and privacy settings are at an appropriate level.
- Make your passwords complex! The passwords used for e-mail, online banking, and other transactions that contain private information should not be simple or easily guessed. The best passwords are a blend of special characters, numbers, and lower and uppercase letters.

Our motto regarding private information must be: ***If we collect it, we must protect it!***

Doris Lama is the Department of the Navy's Freedom of Information Act and Privacy Act policy officer. Richard Wolfe is responsible for privacy in the information assurance/identity management/privacy section of the DON Chief Information Officer. CHIPS

TEN RULES To Protect Personal Information

- DO NOT be afraid to challenge "anyone" who asks to see Privacy Act information that you are responsible for.
- DO NOT maintain records longer than permitted under records disposal.
- DO NOT destroy records before disposal requirements are met.
- DO NOT place unauthorized documents in Privacy Act record systems.
- DO NOT co-mingle information about different individuals in the same file.
- DO NOT transmit personal data without ensuring it is properly marked. Use "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE."
- DO NOT use interoffice envelopes to mail privacy data.
- DO NOT place privacy data on shared drives, multi-access calendars, the Intranet or Internet that can be accessed by individuals who do not have an official need to know.
- DO NOT create a new system of records without first consulting your privacy office or Chief of Naval Operations (DNS-36).
- DO NOT hesitate to offer recommendations on how to better effectively manage privacy data.

– DON Privacy Office

First CTN "A" School Launches at CID Corry Station

By Darlene Goodwin

The first class of the new Cryptologic Technician Networks "A" School convened at the Center for Information Dominance (CID) Corry Station, Feb. 26. Ten Sailors in paygrades E-1 through E-3 are enrolled in the course to learn basic network and networking fundamentals, including devices, topology and security issues.

CID Commanding Officer Capt. Kevin R. Hooley said the training prepares Sailors for complex and mission critical computer network operations in the information warfare domain.

"Information warfare is integral to 21st century Naval operations — combat, peacekeeping, stability and humanitarian," Hooley said. "This course prepares Sailors for these duties in the ever-growing cyber battlespace."

The CTN rating was originally manned with Sailors selected to convert from other CT ratings. Following several rounds of CT-only conversions, the rating is now open to Sailors in any rating who qualify and pass the review process. The first CTN "A" School students are also the first new CTN accessions into the Navy. Cryptologic Technician Networks Seaman Recruit (CTNSR) Casey Denton called it an "amazing milestone" to be a part of.

"CTNs in the future will look to us as pioneers (who built) the pathway they will follow," Denton said. "It is a huge responsibility that we have agreed to take on, and we are all ready and willing to stand up to the challenge."

According to Hooley, the new rating and training were developed in response to emergent warfare requirements and to pace ever advancing technology.

"This evolution bears witness to the dynamic and rapidly responsive nature of our manpower, personnel, training and education system and the Navy's revolution in training," he said. "Combatant commanders and national authorities stated the need for warfare expertise in cyberspace, and in very short order, this new rating was established and formal training implemented."

Course instructor CTN1 (AW) Michael Hawley says the Navy can expect a great product from the new "A" school. "Our goal is to provide the fleet with a Sailor that can make an immediate impact," Hawley said. "And, we fully intend to reach our goal."

CTN "A" School student CTNSR Nancy Pugh is ready to help make that happen. Expressing appreciation to the Navy and nation for the opportunity she has been given, she said, "I'm very proud to be where I am now, knowing that my possibilities are endless, (having been) selected and entrusted to serve the U.S. Navy as a CTN."

CTN "A" School students prepare to begin their new course at the CID Corry Station. Photo by Darlene Goodwin. For related news about the CID, visit the command's Navy NewsStand page at "http://www.news.navy.mil/local/corry/."

Darlene Goodwin is the CID public affairs officer. CHIPS

ThinkTEC Homeland Security Innovation Conference

By Susan Piedfort

SPAWAR Systems Center Charleston participates in conference designed to bring together leaders from industry, science and technology — and the departments of Defense and Homeland Security to advance public and private partnerships.

The 2007 ThinkTEC Homeland Security Innovation Conference provided a first-hand look at new technological advances that enable the warfighter and protect the homeland. The event, sponsored by the Charleston S.C., Metro Chamber of Commerce, was held at the Space and Naval Warfare Systems Center (SSC) Charleston Feb. 21-23.

The goal of the conference was to accelerate the growth of high-tech and knowledge-based business in the region, and to showcase public and private partnership initiatives, technological advances and business opportunities for homeland security and business continuity planning.

The conference was attended by more than 400 leaders from the Navy and departments of Defense and Homeland Security, as well as representatives from technology, science, business and economic development. The conference featured more than 50 exhibits and demonstrations of innovative thinking that result in products for the warfighter and homeland security.

According to James Ward, executive director of SSC Charleston, the conference came at just the right time. "We are showing how we can ensure the safety and enablement of the warfighter, which affects everyone. Everyone is involved in the global war on terrorism," he said. "This is a great opportunity to connect with our peers…"

The conference featured international, national and regional briefings on suicide terrorism, transportation security, Department of Homeland Security (DHS) initiatives, Project Seahawk, infrastructure and disaster planning, and environmental hazards and recovery methods.

Bob Quinn, director of port and maritime security programs for the Oak Ridge National Laboratory, joined Frank Gutierrez, deputy director for Project Seahawk, to discuss an integrated detection system.

Project Seahawk, based in Charleston, is the nation's first collaborative counter-terrorism program set up to identify and respond to potential threats in U.S. waters and ports. Gutierrez, a former naval intelligence officer, discussed how local, state and federal task forces share information to protect ports from terrorist threats.

The conference format was a mix of featured speakers, panel discussions and hands-on exhibits and demonstrations. The event started with a pre-conference day of VIP tours. Attendees toured Charleston Air Force Base, and some got a bird's eye view of Charleston during a C-17 ride. After remarks by U.S. Sen. Jim DeMint (R-S.C.), conference attendees looked at ballistic- and blast-proof vehicles while touring force protection security options in nearby Ladson.

The next two days included presentations, reports from political leaders, networking opportunities and exhibits of cutting-edge technologies.

The Honorable Jay Cohen, a retired Navy rear admiral who now serves as the DHS Under Secretary for Science and Technology, delivered the keynote address. He praised SSC Charleston's success in the delivery of enhanced technology capabilities to the warfighter and to DHS.

In his discussion of future DHS initiatives, Cohen stressed the importance of innovation for the technological advances necessary to ensure mission success.

The former submariner pointed to the Confederate submarine H.L. Hunley as an example. "The Hunley started out as a boiler in Mississippi and was transformed into a warship," said Cohen, whose last tour in the Navy was as Chief of Naval Research. "The innovation you bring is often borne of necessity," he said.

Noting that terrorists take our technology and use it against us, Cohen said we must not only understand technology but also anticipate how it might be abused.

Panel discussions centered on business continuity planning for a disaster; business opportunities and collaboration; and disaster response and recovery.

Demonstrations and exhibits on the "Innovation Isle" featured a radio-controlled helicopter; binoculars which can provide wireless communication on the battlefield; and a video camera which can detect radioactive material.

Conference attendees were exposed to a variety of innovative systems all built for one purpose — to keep the warfighter and nation safe.

Susan Piedfort is the editor of The Chronicle, a magazine published for SSC Charleston employees. For more information about SSC Charleston, go to http://sscc.spawar.navy.mil.

CHIPS

The Honorable Jay Cohen, Under Secretary for Science and Technology, Department of Homeland Security delivering the keynote address of the ThinkTEC Homeland Security Innovation Conference. Cohen is a retired Navy rear admiral whose last tour in the Navy was as Chief of Naval Research. Photo by Harold Senn.

The DON IT Umbrella Program Leads the Way in Savings

It was June 18, 1988, when the Assistant Secretary of the Navy for Financial Management chartered the establishment of the Department of the Navy Information Technology (DON IT) Umbrella Program with acquisition approval authority designated by the Assistant Secretary of the Navy Research, Development and Acquisition and the Chief of Naval Operations.

Since 1988, the Umbrella Program has assisted the Department of Defense (DoD) and DON in making efficient use of IT dollars. The Umbrella Program provides management, technical expertise and financial resources to support the timely and cost effective placement of acquisition vehicles for hardware, software and services. The Umbrella Program team provides full service from contract conception to the end of contract life.

The team collects and analyzes requirements from you, our customers, and assists with preparation of life cycle documents, Request for Proposal/Request for Quote (RFP/RFQ) and source selection. What's more, we ensure that the products and services under the Umbrella Program comply with DON and DoD IT policies. After contracts have been awarded, our project managers continue to provide world-class customer service.

The Umbrella Program is a member of the DON Enterprise Licensing team, which provides support to the Enterprise Software Initiative and SmartBUY programs. ESI is a joint project designed to implement a true software enterprise management process within the Department of Defense. By pooling commercial software requirements and presenting a single negotiating position to leading software vendors, ESI provides pricing advantages not otherwise available to individual services and agencies.

Agreement negotiations and contracting actions are performed by IT acquisition and contracting professionals within participating DoD services and agencies as software project managers (SPM). Go to the ESI Web site for detailed information at http://www.esi.mil.

The ESI is implementing SmartBUY for DoD. SmartBUY is an initiative of the federal government to support effective enterprise level software management. The General Services Administration is designated as executive agent in coordination with the Office of Management and Budget. Its purpose is to consolidate the purchasing power of the federal government by combining volume requirements to obtain optimal pricing and preferred terms and conditions for widely used commercial-off-the-shelf software.

Easy Shopping

Through the ITEC Direct storefront, available at http://www.itec-direct.navy.mil, customers can make direct purchases using the government credit card; contact SPMs and obtain customer service; browse our product line; review policy notices; and access small business contracts.

ITEC Direct offers easy to use point and click shopping to great values on the items you need most. But the DON IT Umbrella Program is so much more than just a convenient way to order hardware, software, office products and services.

Agile business systems and net-centric operations require robust, integrated standards-compliant tools, and that's what the Umbrella Program delivers. The Umbrella Program combines the systematic business strategies of the DoD and DON into a customer friendly solution that means big savings for you in both time and money.

As a key component of the ESI, the Umbrella Program fulfills the Navy's duties as the executive agent for office automation tools, enterprise resource planning (ERP) software and enterprise application integration software.

ESI product agreements include: the entire Microsoft product line; Section 508 tools; Adobe; Oracle; Novell; TOWER Software; Business Objects' Crystal Reports and Crystal Enterprise; Telelogic; NetIQ; Symantec; Quest Software; Red Hat Linux; WinZip; Gartner Research and Advisory Services; IBM; BEA; SAP; and COTS system integration.

Policy Guidance

In addition to each service component's implementing guidance and policy, the Defense Acquisition Regulation Supplement (DFARS) Subpart 208.74 provides policy and procedural guidance. In addition, the recent reissue of the Defense Acquisition System Policy (DoD 5000 series) mandates the leveraging of, and coordination with the DoD ESI when the use of commercial IT is considered viable.

Other guidance includes the policy memo, "DoD Support for the SmartBUY Initiative," issued Dec. 22, 2005, which spells out specific procedures for all DoD in regard to purchasing licenses for commercial software. Finally, relevant provisions of the DoD

DON IT Umbrella Program manager Linda Greenwade (standing) and contract specialist, Sylvia Johnson, from the Information Management (IM)/Information Technology (IT) Department of Naval Inventory Control Point, Mechanicsburg, respond to questions from the audience at the DON IM and IT Conference Umbrella Program Update in February. The Umbrella Program team will deliver another program update at the DON IM and IT Conference to be held at the Virginia Beach Convention Center June 18-21, 2007, in Virginia Beach, Va. See the CHIPS back cover for details.

The DON IT Umbrella Program delivers the best terms and conditions for purchasing COTS products. Don't be fooled by prices that may appear cheaper, but are actually not once you have reviewed the terms and conditions!

Chief Information Officer Guidance and Policy Memorandum of July 26, 2000, may also be incorporated into software directives and instructions.

Ordering is decentralized, but contracting officers can contact the procuring contracting officer or project manager identified on the Umbrella Program Web site at http://www.it-umbrella.navy.mil or in the body of the contract or BPA for assistance.

If you have a requirement for software that is not on the ESI list of "Designated Software," but think it is a good candidate for a DoD-wide Enterprise Software Agreement, you can submit your recommendation via the ESI Web site at http://www.esi.mil. We welcome your feedback!

Periodically, the Umbrella team hears from our customers that they can find products on the DON IT Umbrella Program vehicles for less money by using other purchasing methods. However, we usually find that when the vehicle terms and conditions are reviewed that you can't beat the Umbrella Program prices. Make sure that when you are reviewing terms and conditions that you are comparing apples to apples in a cost comparison. Terms and conditions are a significant factor in pricing!

For example, the ESI has terms that allow transferability within the user base. In this way, software which is no longer needed by the purchasing organization can be redeployed to other organizations within the DON or DoD. The DoD and DON can reap substantial cost avoidance savings by sharing assets within its organizations. Software asset management is something that the DON and DoD are pursuing, and our terms and conditions allow that tracking.

In other cases, maybe the warranty period is longer than a lower priced product vendor. There can be many details that influence price, and it is best to understand those by talking with the cognizant project manager. Your feedback helps us in our research and future discussions with vendors. Vendors in the Umbrella Program are selected by various methods: competition, the sales model of the original equipment manufacturer, e.g., direct sales, reseller or distributor models, and more.

The Umbrella Program is also the proud sponsor of CHIPS, the DON's information technology magazine, celebrating its 25th anniversary this year, and the DON IT Umbrella Program Web site. Both are valuable resources for you. The Umbrella Web site contains purchasing guidance and information about the products and vendors in the Umbrella program.

We are continuously reviewing requirements, which we receive from DoD to determine the products you need most, so please call us for assistance with all your IT needs.

Thank you for allowing us to serve you!

Resources

DON IT Umbrella Program: http://www.it-umbrella.navy.mil

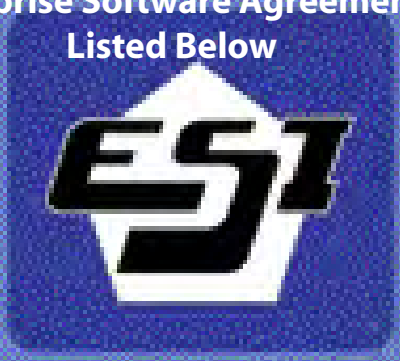
ITEC Direct: http://www.itec-direct.navy.mil

ESI: http://www.esi.mil

CHIPS: http://www.chips.navy.mil

Software Product Manager (SPM)	Contract Vehicle	Savings off GSA Schedule
Linda Greenwade	Microsoft	Up to 38%
	SAP	3 – 19%
	COTS Integration Service Providers	10 – 20%
Peggy Harpe	Oracle (Navy only)	64 – 70%
	Novell	48%
	Telelogic	Up to 15%
	Digital Systems Group IFMIS	Up to 15%
	Gartner	Up to 4%
	HiSoftware 508 Tools	3 – 43%
Sandy Sirbu	RWD	5 – 51%
	iGrafx	21 – 69%
	ITSS	Up to 21.6%
	DON ES	3.5%
Steve Thompson	BEA	Up to 18%
	Adobe	Up to 60% off Transitional Licensing Program (TLP) Level 1
Ted Wolken	TAC	2%

Enterprise Software Agreements Listed Below



The **Enterprise Software Initiative (ESI)** is a Department of Defense (DoD) initiative to streamline the acquisition process and provide best-priced, standards-compliant information technology (IT). The ESI is a business discipline used to coordinate multiple IT investments and leverage the buying power of the government for commercial IT products and services. By consolidating IT requirements and negotiating Enterprise Agreements with software vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in IT acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute and manage IT from the enterprise level.

Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 500.2 in May 2003.

Unless otherwise stated authorized ESI users include all DoD components, and their employees including Reserve component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA nor other IC employees unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.esi.mil/.

Software Categories for ESI:

Business and Modeling Tools

BPWin/ERWin

BPWin/ERWin - Provides products, upgrades and warranty for ERWin, a data modeling solution that creates and maintains databases, data warehouses and enterprise data resource models. It also provides BPWin, a modeling tool used to analyze, document and improve complex business processes.

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002)
Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Business Intelligence

Business Objects

Business Objects - Provides software licenses and support for Business Objects, Crystal Reports, Crystal Enterprise and training and professional services. Volume discounts range from 5 to 20 percent for purchases of software licenses under a single delivery order.
Contractor: ***EC America, Inc.*** (SP4700-05-A-0003)
Ordering Expires: 04 May 10
Web Link: http://www.gsaweblink.com/esi-dod/boa/

Mercury

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: ***Spectrum Systems, Inc.*** (SP4700-05-A-0002)
Ordering Expires: 21 Feb 09
Web Link: http://www.spectrum-systems.com/contracts-ESI.htm

Collaborative Tools

Envoke Software (CESM-E)

Envoke Software - A collaboration integration platform that provides global awareness and secure instant messaging, integration and interoperability between disparate collaboration applications in support of the DoD's Enterprise Collaboration Initiatives.

Contractor: ***Structure Wise*** (DABL01-03-A-1007)
Ordering Expires: 17 Dec 11
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Database Management Tools

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 57.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact Navy project managers on the next page for further details.
Contractors:
DLT Solutions (W91QUZ-06-A-0002)
Mythics, Inc. (W91QUZ-06-A-0003)
Ordering Expires:
DLT: 31 Mar 07 (Call for extension information.)
Mythics: 18 Mar 07 (Call for extension information.)
Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Special Note to Navy Users: On Oct. 1, 2004, and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) San Diego DON Information Technology (IT) Umbrella Program Office.

The Navy Oracle Database Enterprise License provides significant benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/deal/Oracle/oracle.shtml

Sybase (DEAL-S)

Sybase Products - Offers a full suite of software solutions designed to assist customers in achieving Information Liquidity. These solutions are focused on data management and integration; application integration; Anywhere integration; and vertical process integration, development and management. Specific products include but are not limited to: Sybase's Enterprise Application Server; Mobile and Embedded databases; m-Business Studio; HIPAA (Health Insurance Portability and Accountability Act) and Patriot Act Compliance; PowerBuilder; and a wide range of application adaptors. In addition, a Golden Disk for the Adaptive Server Enterprise (ASE) product is part of the agreement. The Enterprise portion of the BPA offers NT servers, NT seats, Unix servers, Unix seats, Linux servers and Linux seats. Software purchased under this BPA has a perpetual software license. The BPA also has exceptional pricing for other Sybase options. The savings to the government is 64 percent off GSA prices.

Contractor: ***Sybase, Inc.*** (DAAB15-99-A-1003); (800) 879-2273; (301) 896-1661
Ordering Expires: 15 Jan 08
Authorized Users: Authorized users include personnel and employees of the DoD, Reserve components (Guard and Reserve), U.S. Coast Guard when mobilized with, or attached to the DoD and nonappropriated funds instrumentalities. Also included are Intelligence Communities, including all DoD Intel Information Systems (DoDIIS) member organizations and employees. Contractors of the DoD may use this agreement to license software for performance of work on DoD projects.

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Application Integration

BEA - NEW!

BEA Products - Supplies integration and service-oriented architecture (SOA) software including: BEA WebLogic Server; BEA WebLogic Portal; BEA WebLogic Integration; BEA WebLogic Workshop; BEA JRockit; BEA AquaLogic; BEA Tuxedo and other BEA products.

Contractors:
CompSec (Computer Security Solutions, Inc.) (N00104-07-A-ZF43); Small Business; (703) 917-0382
immixTechnology, Inc. (N00104-07-A-ZF41); Small Business; (703) 752-0659
Merlin International (N00104-07-A-ZF42); Small Business; (703) 752-8369
Ordering Expires: 19 Dec 09

Web Links:
CompSec
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/CompSec/index.shtml
immixTechnology
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/immix/index.shtml
Merlin International
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/Merlin/index.shtml

Enterprise Architecture Tools

IBM Software Products

IBM Software Products - Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products including IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

Contractor: ***immixTechnology, Inc.*** (DABL01-03-A-1006); Small Business; (800) 433-5444
Ordering Expires: 26 Mar 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS2)

Computer Associates Unicenter Enterprise Management Software - Includes Security Management; Network Management; Event Management; Output Management; Storage Management; Performance Management; Problem Management; Software Delivery; and Asset Management. In addition to these products there are many optional products, services and training available.

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002); (800) 645-3042
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Citrix

Citrix - Provides a full range of Metaframe products including Secure Access Manager, Conferencing Manager, Password Manager, Access Suite & XP Presentation Server. Discounts range from 2 to 5 percent off GSA Schedule pricing plus spot discounts for volume purchases.
Contractor: ***Citrix Systems, Inc.*** (W91QUZ-04-A-0001); (772) 221-8606
Ordering Expires: 23 Feb 08
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Microsoft Premier Support Services (MPS-1)

Microsoft Premier Support Services - Provides premier support packages to small and large-size organizations. The products include Technical Account Managers, Alliance Support Teams, Reactive Incidents, on-site support, Technet and MSDN subscriptions.

Contractor: ***Microsoft*** (DAAB15-02-D-1002); (980) 776-8283
Ordering Expires: 30 Jun 07
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

NetIQ

NetIQ - Provides Net IQ systems management security management and Web analytics solutions. Products include: AppManager; AppAnalyzer; Mail Marshal; Web Marshal; Vivinet voice and video products; and Vigilant Security and Management products. Discounts are 10 to 8 percent off GSA Schedule pricing for products and 5 percent off GSA Schedule pricing for maintenance.

Contractors:
NetIQ Corp. (W91QUZ-04-A-0003)
Northrop Grumman - authorized reseller
Federal Technology Solutions, Inc. - authorized reseller
Ordering Expires: 5 May 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The software product provides the enterprise with a suite of solution specific applications for Capital Planning and Investment Control (CPIC) Budgeting (OMB 300/53); CPIC Process (Select/Control/Evaluate); IT Governance; FISMA (Federal Information Security Management Act) and Privacy Compliance; Project Portfolio Management; Application Rationalization; Research and Development (R&D) and Product Development; Asset Management; Grants Management; Vendor and Service Level Agreement Management; and Regulatory Compliance. ProSight products have been designated as a DoD ESI and GSA SmartBUY. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014); (503) 889-4813
Ordering Expires: 31 Dec 07 (Call for extension information. Currently in review for extension.)
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Quest Products

Quest Products - Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. Active Directory Products only have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.

Contractors:
Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800
DLT Solutions (W91QUZ-06-A-0004); (703) 709-7172
Ordering Expires:
Quest: 14 Aug 10
DLT: 31 Mar 07 (Call for extension information.)
Web Links:
Quest
https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023
DLT
https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-06-A-0004

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development life cycle. The major products include DOORS, SYNERGY and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:
Bay State Computers, Inc. (N00104-04-A-ZF13); Small Business Disadvantaged; (301) 352-7878, ext. 116
Spectrum Systems, Inc. (N00104-06-A-ZF31); Small Business ; (703) 591-7400
Ordering Expires: 29 Jun 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/telelogic/telelogic.shtml

Enterprise Resource Planning

Digital Systems Group

Digital Systems Group - Provides Integrated Financial Management Information System (IFMIS) software that was designed specifically as federal financial management system software for government agencies and activities. The BPA also provides installation, maintenance, training and professional services.

Contractor: ***Digital Systems Group, Inc.*** (N00104-04-A-ZF19); (215) 443-5178
Ordering Expires: 23 Aug 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/dsg/dsg.shtml

Oracle

Oracle - *See information provided under Database Management Tools on page 53.*

RWD Technologies

RWD Technologies - Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.

Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (410) 869-1085
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/rwd/rwd.shtml

SAP

SAP Software - Provides software license, installation, implementation technical support, maintenance and training services.

Contractor: ***SAP Public Sector & Education, Inc.*** (N00104-02-A-ZE77); (202) 312-3905
Ordering Expires: Effective for term of the GSA FSS Schedule
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/sap/sap.shtml

ERP Systems Integration Services

ERP Systems

ERP Systems Integration Services - Provides the procurement of configuration; integration; installation; data conversion; training; testing; object development; interface development; business process reengineering; project management; risk management; quality assurance; and other professional services for COTS software implementations. Ordering under the BPAs is decentralized and is open to all DoD activities. The BPAs offer GSA discounts from 10 to 20 percent. Firm fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA Schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Contractors:
Accenture LLP (N00104-04-A-ZF12); (703) 947-2059
BearingPoint (N00104-04-A-ZF15); (703) 747-5442
Computer Sciences Corp. (N00104-04-A-ZF16); (856) 252-5583
Deloitte Consulting LLP (N00104-04-A-ZF17); (703) 885-6428
IBM Corp. (N00104-04-A-ZF18); (301) 803-6625
Ordering Expires: 03 May 09
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml

Information Assurance Tools

Network Associates, Inc.

Network Associates, Inc. (NAI) - This protection encompasses the following NAI products: VirusScan; Virex for Macintosh; VirusScan Thin Client; NetShield; NetShield for NetApp; ePolicy Orchestrator; VirusScan for Wireless; GroupShield; WebShield (software only for Solaris and SMTP for NT); and McAfee Desktop Firewall for home use only.

Contractor: ***Network Associates, Inc.*** (DCA100-02-C-4046)
Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.
Web Link: http://www.esi.mil
Antivirus Web Links: Antivirus software available for no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Securify

Securify - Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. Securify integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.

Contractor: ***Patriot Technologies, Inc.***
Ordering Expires: 4 Jan 11 (if extended by option exercise)
Web Link: http://www.esi.mil

Symantec

Symantec - Provides the full line of Symantec Corp. products and services consisting of over 6,000 line items including Ghost and Brightmail. Symantec products can be divided into eight main categories that fall under the broad definition of Information Assurance. These categories are: virus protection; anti-spam; content filtering; anti-spyware solutions; intrusion protection; firewalls/VPN; integrated security; security management; vulnerability management; and policy compliance. ***Notice to DoD customers regarding Symantec Antivirus Products:*** *A DoD Enterprise License exists for select Antivirus products through DISA contract DCA100-02-C-4049 found below.*
Contractor: ***immixTechnology, Inc.***
Ordering Expires: 12 Sep 10
Web Link: http://www.immixtechnology.com/esi/Symantec/ or http://www.esi.mil

Symantec Antivirus

Symantec - This protection encompasses the following Symantec products: Symantec Client Security; Norton Antivirus for Macintosh; Symantec System Center; Symantec AntiVirus/Filtering for Domino; Symantec AntiVirus/Filtering for MS Exchange; Symantec AntiVirus Scan Engine; Symantec AntiVirus Command Line Scanner; Symantec for Personal Electronic Devices; Symantec AntiVirus for SMTP Gateway; Symantec Web Security (AV only); and support.
Contractor: ***Northrop Grumman Information Technology*** (DCA100-02-C-4049)
Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.
Web Link: http://www.esi.mil
Antivirus Web Links: Antivirus software available for no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Trend Micro

Trend Micro - This protection encompasses the following Trend Micro products: InterScan Virus Wall (NT/2000, Solaris, Linux); ScanMail for Exchange (NT, Exchange 2000); TMCM/TVCS (Management Console - TMCM W/OPP srv.); PC-Cillin for Wireless; and Gold Premium support contract/year (PSP), which includes six POCs.

Contractor: ***Government Technology Solutions*** (DCA100-03-C-4011)
Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.
Web Link: http://www.esi.mil
Antivirus Web Links: Antivirus software available for no cost; download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Xacta

Xacta - Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555
Ordering Expires: 31 Jul 08
Web Link: http://esi.telos.com/contract/overview/

Office Systems

Adobe

Adobe Products - Provides software licenses (new and upgrade) and upgrade plans (formerly known as maintenance) for numerous Adobe and formerly branded Macromedia products, including Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion and other Adobe products.

Contractors:
ASAP (N00104-06-A-ZF33); Small Business; (800) 248-2727, ext. 5303
CDW-G (N00104-06-A-ZF34); (703) 621-8211
Softchoice (N00104-06-A-ZF35); Small Business; (703) 480-1957
Softmart (N00104-06-A-ZF36); Small Business; (610) 518-4192
Ordering Expires: 31 May 08
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe-esa/index.shtml

Four Blanket Purchase Agreements (BPAs) provide both new and upgrade software licenses for Adobe products. These agreements also provide Adobe software upgrade plans, formerly known as maintenance agreements. The BPAs include software licenses formerly known under the Macromedia product brand. Products include: Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion; and other Adobe products.

iGrafx Business Process Analysis Tools

iGrafx - Provides software licenses, maintenance and media for iGrafx Process 2005 and 2006 for Six Sigma and iGrafx Flowcharter 2005 and 2006.

Contractors:
Softchoice (N00104-06-A-ZF40); (703) 480-1957
Softmart (N00104-06-A-ZF39); (610) 518-4192
Software House International (N00104-06-A-ZF38); (732) 868-5916
Authorized Users: Open for ordering by all Department of Defense (DoD) Components, U. S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.
Ordering Expires: 16 Jul 08
Web Links:
Softchoice
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softchoice/index.shtml
Softmart
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softmart/index.shtml
Software House International
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/shi/index.shtml

Microsoft Products

Microsoft Products - Provides licenses and software assurance for desktop configurations, servers and other products. In addition, any Microsoft product available on the GSA Schedule can be added to the BPA.

Contractors:
ASAP (N00104-02-A-ZE78); Small Business; (800) 248-2727, ext. 5303
CDW-G (N00104-02-A-ZE85); (847) 968-9429
Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 37010 or (512) 723-7010
GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 463-5325
Hewlett-Packard (N00104-02-A-ZE80); (800) 535-2563 pin 6246
Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (312) 655-9167
Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928
Software House International (N00104-02-A-ZE86); (732) 868-5926
Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2208
Ordering Expires: 30 Mar 07 (Call for extension information.)
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Red Hat

Red Hat *(Netscape software formerly owned by AOL, not Linux)* - In December 2004, America Online (AOL) sold Netscape Security Solutions Software to Red Hat. This sale included the three major software products previously provided by DISA (Defense Information Systems Agency) to the DoD and Intelligence Communities through AOL. *Note: The Netscape trademark is still owned by AOL, as are versions of Netscape Communicator above version 7.2. Netscape Communicator version 8.0 is not part of this contract.*

August Schell Enterprises is providing ongoing support and maintenance for the Red Hat Security Solutions (products formerly known as Netscape Security Solutions) which are at the core of the DoD's Public Key Infrastructure (PKI). This contract provides products and services in support of the ongoing DoD-wide enterprise site license for Red Hat products. This encompasses all components of the U.S. Department of Defense and supported organizations that use the Joint Worldwide Intelligence Communications System (JWICS), including contractors.

Licensed software products available from DISA are the commercial versions of the software, not the segmented versions that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a licensed product available for download from the DoD Download Site to support development or operation of an application associated with the GIG, GCCS or GCSS, you must contact one of the Web sites listed below to obtain the GIG segmented version of the software. You may not use the commercial version available from the DoD Download Site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the Web sites listed below for additional information to help you to make this determination before you obtain the software from the DoD Download Site.

GIG or GCCS users: Common Operating Environment Home Page
https://coe.mont.disa.mil
GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

Contractor: ***August Schell Enterprises***
Ordering Expires: 06 Mar 07 (Call for extension information)
Download provided at no cost.
Web Link: http://iase.disa.mil/netlic.html

Red Hat Linux

Red Hat Linux - Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractor: ***DLT Solutions, Inc.*** (HC1013-04-A-5000)
Ordering Expires: 30 Apr 09
Web Link: http://www.dlt.com/contracts-Redhat-BPA.asp

WinZip

WinZip - This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip 9.0, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses. All customers are entitled to free upgrades and maintenance for a period of two years from original purchase. Discount is 98.4 percent off retail. Price per license is 45 cents.

Contractor: ***Eyak Technology, LLC*** (W91QUZ-04-D-0010)
Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY Contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Ordering Expires: 27 Sep 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Operating Systems

Novell

Novell Products - Provides master license agreement for all Novell products, including NetWare, GroupWise and ZenWorks.

Contractor: ***ASAP Software*** (N00039-98-A-9002); Small business; (800) 883-7413
Ordering Expires: 30 Jun 07
Web Link:
http://www.it-umbrella.navy.mil/contract/enterprise/novell/novell.shtml

Sun (SSTEW)

SUN Support - Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)
Ordering Expires: Dependent on GSA Schedule until 2011
Web Link: http://www.ditco.disa.mil/hq/contracts/sstewchar.asp

Research and Advisory BPA

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006
Ordering Expires: 30 Mar 08
Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.
Web Link: http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

Records Management

TOWER Software

TOWER Software - Provides TRIM Context software products, maintenance, training and services. TRIM Context is an integrated electronic document and records management platform for Enterprise Content Management that securely manages business information in a single repository through its complete life cycle. The TOWER TRIM solution provides: document management; records management; workflow management; Web-based records management; document content indexing; e-mail management; and imaging. The DoD Enterprise Software Initiative (ESI) Enterprise Software Agreement (ESA) provides discounts of 10 to 40 percent off GSA for TRIM Context software licenses and maintenance and 5 percent off GSA for training and services.

Contractor: ***TOWER Software Corporation*** (FA8771-06-A-0302)
Ordering Expires: 17 Feb 08 (5 Dec 10 if extended by option exercise)
Web link: http://www.esi.mil

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools - Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage, AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

Contractor: ***HiSoftware, DLT Solutions, Inc.*** (N00104-01-A-Q570); Small Business; (888) 223-7083 or (703) 773-1194
Ordering Expires: 15 Aug 07
Web Link: http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.shtml
Warranty: IAW GSA Schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

ViViD Contracts
N68939-97-D-0040
Contractor: Avaya Inc.
N68939-97-D-0041
Contractor: General Dynamics

ViViD provides digital switching systems, cable plant components, communications and telecommunications equipment and services required to engineer, maintain, operate and modernize base level and ships afloat information infrastructure. This includes pierside connectivity and afloat infrastructure with purchase, lease and lease-to-own options. Outsourcing is also available. Awarded to:

Avaya Inc. (N68939-97-D-0040); (888) VIVID4U or (888) 848-4348. Avaya also provides local access and local usage services
General Dynamics (N68939-97-D-0041); (888) 483-8831
Modifications: Latest contract modifications are available at http://www.it-umbrella.navy.mil
Ordering Expires:
Contract ordering for all new equipment purchases has expired. All Labor CLINS, Support Services and Spare Parts can still be ordered through 28 Jul 07.
Authorized users: DoD and U.S. Coast Guard
Warranty: Four years after government acceptance. Exceptions are original equipment manufacturer (OEM) warranties on catalog items.
Acquisition, Contracting & Technical Fee: Included in all CLINs/SCLINs
Direct Ordering to Contractor
Web Link: http://www.it-umbrella.navy.mil/contract/vivid/vivid.shtml

TAC Solutions BPAs
Listed Below

TAC Solutions provides PCs, notebooks, workstations, servers, networking equipment and all related equipment and services necessary to provide a completely integrated solution. BPAs have been awarded to the following:

Dell (N68939-97-A-0011); (800) 727-1100, ext. 7233795
GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104
Hewlett-Packard (N68939-96-A-0005); (800) 727-5472, ext. 15614
Ordering Expires:
Dell: 31 Mar 07 (Call for extension information.)
GTSI: 31 Mar 07 (Call for extension information.)
Hewlett-Packard: 07 May 07 (Call for extension information.)
Authorized Users: DON, U.S. Coast Guard, DoD and other federal agencies with prior approval.
Warranty: IAW GSA Schedule. Additional warranty options available.

Web Links:
Dell
http://www.it-umbrella.navy.mil/contract/tac-solutions/dell/dell.shtml
GTSI
http://www.it-umbrella.navy.mil/contract/tac-solutions/gtsi/gtsi.shtml
Hewlett-Packard
http://www.it-umbrella.navy.mil/contract/tac-solutions/HP/HP.shtml

Department of the Navy Enterprise Solutions BPA
Navy Contract: N68939-97-A-0008

The Department of the Navy Enterprise Solutions (DON ES) BPA provides a wide range of technical services, specially structured to meet tactical requirements, including worldwide logistical support, integration and engineering services (including rugged solutions), hardware, software and network communications solutions. DON ES has one BPA.

Computer Sciences Corp. (N68939-97-A-0008); (619) 225-2600; Awarded 7 May 97

Ordering Expires: 31 Mar 07 (Call for extension information.)

Authorized Users: All DoD, federal agencies and U.S. Coast Guard.

Web Link: http://www.it-umbrella.navy.mil/contract/don-es/csc.shtml

Information Technology Support Services BPAs
Listed Below

The Information Technology Support Services (ITSS) BPAs provide a wide range of IT support services such as networks, Web development, communications, training, systems engineering, integration, consultant services, programming, analysis and planning. ITSS has four BPAs. They have been awarded to:

Centurum Information Technology, Inc. (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98

Lockheed Martin (N68939-97-A-0017); (703) 367-3407; Awarded 1 Jul 97

Northrop Grumman Information Technology (N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97

SAIC (N68939-97-A-0020); (858) 826-5899; Awarded 1 Jul 97

Ordering Expires:
Centurum: 14 Jul 07 (Call for extension information.)
Lockheed Martin: 30 Jun 07 (Call for extension information.)
Northrop Grumman IT: 11 Feb 07 (Call for extension information.)
SAIC: 30 Jun 07 (Call for extension information.)

Authorized Users: All DoD, federal agencies and U.S. Coast Guard

Web Links:
Centurum
http://www.it-umbrella.navy.mil/contract/itss/centurum/itss-centurum.shtml
Lockheed Martin
http://www.it-umbrella.navy.mil/contract/itss/lockheed/itss-lockheed.shtml
Northrop Grumman IT
http://www.it-umbrella.navy.mil/contract/itss/northrop/itss-northrop.shtml
SAIC
http://www.it-umbrella.navy.mil/contract/itss/saic/itss-saic.shtml

The DON IT Umbrella Program Team offers great customer service!

Visit us on the Web

DON IT Umbrella site:
www.it-umbrella.navy.mil

ITEC Direct e-Commerce site:
www.itec-direct.navy.mil

DoD Enterprise Software Initiative site:
www.esi.mil

DON IT
umbrella program

YOU ARE INVITED TO THE

DON IM and IT Conference

Department of the Navy Information Management and Information Technology

Hosted by the Department of the Navy Chief Information Officer (DON CIO)

18-21 June 2007

Virginia Beach Convention Center, Virginia Beach, VA

The DON IM and IT Conference provides a venue to share information about the latest DON IM and IT initiatives, policy and guidance. Conference topics include:

- Certification & Accreditation
- Critical Infrastructure Protection
- Data Management
- DITPR-DON Training
- DON IM/IT Civilian Workforce
- DON IT Umbrella Program
- Enterprise Architecture
- Enterprise Software/IT Asset Management
- FISMA
- Information Assurance
- IT Performance Measurement
- Knowledge Management in Support of the Warfighter
- Privacy
- Public Key Infrastructure
- Service Oriented Architecture
- Strategic Management of the Electromagnetic Spectrum
- Telecommunications
- USMC Civilian ITM Community of Interest
- WiMAX
- Wireless

The DON IM and IT Conference will be open to all DON, government, military and support contractor attendees. No conference fee will be assessed, but registration is required.

The agenda and registration are available on the DON CIO Web site at http://www.doncio.navy.mil. For additional information call (703) 602-6274 or (703) 607-5650.

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN CHARLESTON
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK, VA 23511 - 2130
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND ADDITIONAL
MAILING OFFICE
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988